

Protecting Privacy for Volunteers

Guide

Protecting the privacy of volunteers

Australian privacy laws are complex. This Fast Facts sheet sets out a summary of the key privacy principles and compliance requirements organisations should follow when managing personal information about their volunteers.

Do I need to comply?

An organisation's legal obligation to comply with privacy laws depends on a number of variables. So which organisations have a duty to protect personal information about a volunteer under privacy laws? The short answer is: it depends on an organisation's individual circumstances.

Whether your organisation is required or not to comply with privacy laws, it is good practice to adopt the principles set out in privacy laws when managing volunteer personal information. You should seek legal advice if you are unsure about whether privacy laws apply to your organisation.

What's it all about: privacy

In Australia, privacy laws focus on the collection and handling of personal information.

Personal information means information or an opinion about a volunteer, whether true or not, and whether recorded in a material form or not, about an identified volunteer or a volunteer who is reasonably identifiable (depending on the applicable law). In other words, if your organisation could use any of the information it collects to identify a volunteer, its personal information.

Examples of personal information include:

- name
- contact details, such as address or phone number
- date of birth
- living arrangements
- bank account details
- employment history
- hobbies, clubs or activities
- photos or videos
- likes and opinions expressed about a volunteer by another person.

Sensitive information is a subset of personal information and includes:

- health information
- genetic information
- biometric information
- criminal history
- religious beliefs or affiliations
- racial or ethnic origin
- sexual orientation or practices
- political opinions
- membership of a political association
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union.

Everybody's business

If your organisation is not mandated by law to comply with privacy laws, Volunteering Victoria recommends that your organisation seeks to comply with privacy laws as a matter of best practice.

There are three main laws relating to the collection and handling of personal information that may apply to Victorian volunteer-involving organisations:

1. Information Privacy Act 2000 (Victoria)

This Act is generally intended to apply to Victorian Government agencies. However, organisations are often required to comply with this Act under the funding agreements with the State of Victoria or where the organisation is contracted to provide services on behalf of a Victorian Government agency.

2. Privacy Act 1988 (Commonwealth)

Applies to organisations with an annual turnover of more than \$3 million, collects Tax File Numbers or receives Commonwealth Government funding. Again organisations are often required to comply with this Act under Commonwealth funding agreements.

3. Health Records Act 2001 (Victoria)

Applies to organisations providing a health, disability or aged care service.

Privacy principles

These privacy principles are a roadmap for good practice in managing the personal information about volunteers. You may be legally obligated to comply with the privacy principles depending on which privacy laws are applicable to you.

Collection

Only collect personal information from a volunteer that is necessary for, or directly related to, one or more of your organisation's functions or activities. An example of an activity is the recruitment of volunteers.

At the time you collect personal information from a volunteer, provide a collection notice to the volunteer that sets out:

- your organisation's name and contact details
- the purpose of the collection of the personal information
- the main consequences (if any) for the volunteer if all or some of the personal information your organisation requests is not provided by the volunteer
- whether your organisation will disclose the personal information to a third party and the names and types of such third parties (including whether the personal information will be disclosed to another organisation located outside of Victoria)
- a link to your organisation's publicly accessible privacy policy (if you have one)
- how a volunteer may gain access to or correct their personal information
- any law requiring the collection

Use and disclosure

Use and disclose a volunteer's information only for the purposes for which it was collected (for example, for checking their references).

Your organisation may have multiple purposes, or for related secondary purposes, for collecting a volunteer's personal information. Your organisation may use or disclose a volunteer's personal information for these multiple purposes, provided your organisation notified the volunteer of these multiple purposes in a collection notice. Obtain the consent from a volunteer before using or disclosing their personal information for any other purpose, unless it is for a related secondary purpose (the secondary purpose must be directly related to the primary purpose of collection for sensitive information).

There may be circumstances where disclosure of a volunteer's personal information without consent is appropriate and legal; for example, if a volunteer poses a danger to themselves or others and sharing their information may prevent harm. If you are about whether you can legitimately use or disclose personal information of a volunteer for a particular purpose, seek advice from your organisation's privacy officer, a privacy authority or legal advice service.

Data quality

Make sure any personal information you hold, use or disclose is accurate, complete and up to date. For example, you may routinely ask volunteers to update their contact details recorded by your organisation.

Data security

Take reasonable steps to protect personal information from misuse, loss and from unauthorised access, modification or disclosure by storing all files securely, whether in hard copy or digital form.

Destroy or de-identify any personal information you have on file if it is no longer needed for any purpose and your organisation does not have a legal requirement to keep a record of the information in an identifiable format.

Openness

Have an accessible, written policy on how you manage personal information (ie a privacy policy). An organisation will usually make its privacy policy available on its website.

Unique identifiers

Avoid using a 'Government related identifier' in volunteer files as your organisation's own volunteer identifier, such as Tax File Numbers and driver license numbers. Organisations can only use Government related identifiers in limited circumstances. Seek advice if you are unsure about whether your organisation can use a volunteer's Government related identifier for a particular purpose.

Crossing borders

When transferring personal information to a recipient located outside of Victoria, ensure that the recipient complies with privacy principles of a similar standard that apply to your organisation. This may involve requiring the recipient to agree to comply with privacy laws under a written agreement, such as a data transfer agreement. You will also need to let volunteers know if you intend on transferring their personal information outside of Victoria.

Sensitive information

Sensitive information should be collected and handled with a higher level of protection than personal information. Generally sensitive information about a volunteer can only be collected with the consent of that volunteer. Sensitive information should only be used and disclosed for purposes that are directly related to the primary purpose of collection. For example, if a volunteer disclosed a pre-existing medical condition to your organisation that limited the volunteer's capacity to complete certain tasks, the organisation could use the information about the volunteer's medical condition to make necessary adjustments to the workplace environment (ie conduct an ergonomic assessment and purchase equipment). This information could not

be used or disclosed for other purposes, for example disclosing the volunteer's pre-existing medical condition to other volunteers who do not have a need to know this information.

Anonymity

Where lawful and practicable, organisations must provide individuals with the option of not identifying themselves when entering into transactions with an organisation. This may not be a practical option when dealing with volunteer personal information as your organisation is likely to need to collect basic identifying information about a volunteer for operational and legal reasons.

Appointing a privacy officer

It is good practice to appoint a dedicated person as a privacy officer within your organisation. The privacy officer will be the first point of contact for internal and external privacy queries and complaints and should assist your organisation with privacy compliance activities. The privacy officer should have an in-depth understanding and knowledge of the privacy laws that apply to your organisation to carry out the privacy officer role effectively.

Privacy impact assessments

A privacy impact assessment is a detailed assessment of a project that identifies the impact a project might have on the privacy of individuals (including volunteers). Completing privacy impact assessments on projects your organisation undertakes that involve the collection and handling of personal information can be a useful way to successfully implement a project in a manner that complies with relevant privacy laws and to identify any privacy risks up front before the project begins or is implemented.

Handling privacy queries and complaints

Your organisation should have a documented process that it follows to deal with privacy queries and complaints. Generally, volunteers will have a right to access and correct their personal information. Your organisation should have a process that allows volunteers to easily request access to or correct the personal information your organisation holds about them. Similarly, volunteers should also be able to lodge a privacy complaint with your organisation easily and receive a response to their complaint within 30 days.

Data breaches

Data breaches are increasingly becoming a common feature of modern day life, with the increasing use of technology and the electronic storage of data.

Your organisation should plan for the occurrence of a data breach and know what to do when a data breach occurs. Your organisation should have a data breach response plan to be able to respond and recover from a data breach effectively and comply with any mandatory data breach notification laws.

More information

This Fast Facts sheet provides a summary of privacy laws that may apply to your organisation and key compliance actions to adopt. It is not intended to be a substitute for seeking legal advice if you have a privacy issue.

There are a number of websites that provide additional information on privacy laws. If you would like more information please visit the websites listed below.

- Office of the Australian Information Commissioner (OAIC) - www.oaic.gov.au
- Office of the Victorian Information Commissioner (OVIC) - www.cdp.vic.gov.au
- Not-for-profit Law - www.nfplaw.org.au/privacy
- Department of Health & Human Services (DHHS) - www2.health.vic.gov.au/about/legislation/health-records-act