Drafting a privacy policy

Guidance for the Victorian public sector

Victorian public sector organisations covered by Part 3 of the *Privacy and Data Protection Act 2014* (**PDP Act**) are required to adhere to 10 Information Privacy Principles (**IPPs**). The IPPs set out the minimum standards for the handling of personal information in the Victorian public sector.[1]

IPP 5 requires an organisation to have a document that clearly sets out its policies on the management of personal information, and to make it available to anyone that asks for it. This document is commonly referred to as a privacy policy.

This information sheet provides general guidance about privacy policies. It is aimed at Victorian public sector organisations that are bound by the PDP Act. This includes local councils and contracted service providers.[2]

What is a privacy policy?

A privacy policy is a general statement about how an organisation manages personal information. It demonstrates the organisation's commitment to privacy by explaining how it adheres to its privacy obligations.

In addition to meeting the requirements of IPP 5, other benefits of having a privacy policy include:

- helping employees understand how personal information should be handled;
- preventing the unnecessary collection or unlawful use or disclosure of information; and
- promoting greater public confidence in the organisation's handling of personal information.

In some cases, depending on the range and diversity of its core functions, an organisation may choose to produce more than one privacy policy. For example, a large department with a number of business units may have multiple privacy policies to cover the department's distinct functions and information handling practices.

Privacy policies and collection notices

Although they both inform individuals about how an organisation will manage their personal information, privacy policies and collection notices are different.

A privacy policy speaks about an organisation's information management practices in a broad sense, whereas a collection notice outlines an organisation's information handling practices for a specific purpose or activity.

For example, when collecting personal information from an individual who is registering their pet, a local council will provide the pet owner with notice about how it will handle that information. This is different to the council's privacy policy, which will outline the council's commitment to information management in a general sense.

For more information about collection notices, please refer to the *Collection notices* information sheet published by OVIC.

[1] Personal information is defined under s 3 of the PDP Act.

[2] A contracted service provider is a person or body who provides services under a State contract.

What should a privacy policy contain?

When drafting a privacy policy, it is important to look at the different ways that the organisation collects personal information, and how that information flows through the organisation.

A privacy policy should consider all the different ways that personal information may be collected – for example, via telephone, websites, or paper-based collection.

General privacy policies do not need to be technology specific, however organisations may wish to include specific sections, or create stand-alone policies, to reflect their use of particular technologies or programs.

For example, a privacy policy may reference an organisation's collection of information from individuals who visit their website and contain a distinct section about how this information is handled; alternatively, organisations may choose to develop a separate website privacy policy.

Privacy policies should reflect an organisation's own authorising environment and operational practices. As such, each organisation's privacy policy will be different.

Organisations may choose to outline their information handling practices by reference to the IPPs. A privacy policy should not simply re-state each of the principles but demonstrate the steps that the organisation takes to adhere to each of the IPPs.

At a minimum, a privacy policy should include:

- the identity of the organisation;
- the organisation's main functions and the types of personal information it generally collects to fulfil those functions;
- how the organisation uses and shares the personal information it collects, including the types of third parties the information may be shared with;
- whether collection of personal information is compulsory or optional (including referring to any relevant legislation that authorises the collection, use or disclosure of the information);
- how the organisation securely stores and manages access to the personal information, and for how long it may be stored;
- how privacy is protected if the information is transferred or stored outside Victoria;
- the date and version of the policy; and
- how an individual can contact the organisation, request access to the information held about them, or make a privacy complaint.

Drafting an effective privacy policy

The underlying principle of IPP 5 is transparency. It is therefore important that privacy policies are clear and easily understandable.

Some ways to ensure an effective privacy policy include:

- **use plain language** – for example, short, clear sentences and familiar, plain English words;
- **avoid legal jargon** or technical terminology;
- **be specific** about the organisation's functions and how it will use the personal information it holds – avoid using general 'catch-all' terms or replicating other organisations' privacy policies;
- **provide sufficient information** – having a concise privacy policy can be effective, however it also needs to contain enough detail to allow individuals to understand how their personal information will be handled; and
- **be user-friendly** – avoid large slabs of text and consider organising the privacy policy into sections with clear headings.

Layering privacy policies

Where appropriate, an organisation may decide to 'layer' its privacy policy. This may involve, for example, providing a brief summary of the organisation's privacy policy on a form, sign, or poster, and then referring, or providing a link to, the full privacy policy. A layered approach informs individuals about the existence of the

organisation's privacy policy and allows them to seek further information if they wish.

Health information

Some organisations may collect and handle health information in addition to other personal information. However, this does not necessarily require two separate privacy policies. The *Health Records Act 2001* contains Health Privacy Principles (**HPPs**) that are similar to the IPPs in the PDP Act. Organisations may prefer to develop one privacy policy that addresses the principles in both Acts.

For more information about the HPPs, organisations should contact the Health Complaints Commissioner.

Publishing a privacy policy

There is no specific requirement under the PDP Act for organisations to publish a privacy policy – only to make it available to anyone who asks for it. However, most organisations will find it practical and cost effective to publish their privacy policy so that it can be easily found by individuals who would like to see a copy.

Some effective ways to make a privacy policy available include:

- featuring the privacy policy on the organisation's website, with appropriate links to more detailed information;
- including a copy of the privacy policy in mail correspondence or providing a web link in emails;
- recording a brief message that telephone callers can choose to hear, or that plays while a caller is on hold; and
- placing a privacy policy prominently at an organisation's reception desk, in a waiting room, or meeting area.

Updating a privacy policy

Privacy policies should be reviewed regularly and updated when necessary to reflect changes in legislation or information management practices.

Further, when an organisation adopts a new program, system or technology, is assigned new functions, or undergoes a restructure, it is worthwhile re-visiting the privacy policy to ensure that it is still up to date and accurately reflects the flow of information through the organisation.

If an organisation begins to collect more information, or uses or discloses information in new ways, this should be immediately reflected in its privacy policy.

Further Information

Contact Us

t: 1300 00 6842
e: enquiries@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

The information in this document is general in nature and does not constitute legal advice.