Office of the Victorian Information Commissioner

IPP 5 – Openness

IPP 5 – Openness

On this page

IPP 5.1: Written policy on management of personal information 3

Publishing the privacy policy 5

Writing a privacy policy 5

Availability of privacy policies 6

Timeframe to provide the privacy policy 7

IPP 5.2: Responding to requests about the sort of information held and how it is used 7

Relationship between IPP 5 and other information handling obligations 8

Frequently asked questions (FAQs) 8

What should a privacy policy contain? 8

What is the difference between a privacy policy, collection notice and consent form? 9

How often should an organisation review its privacy policy? 9

What if an organisation provides different types of services – do they need to have more than one privacy policy? 9

Should an organisation cover health information in their privacy policy? 10

Who should draft a privacy policy? 10

How can an organisation effectively distribute their privacy policy? 10

What if an organisation collects personal information from children – how can they draft a privacy policy for a young audience? 10

Version control table 11

IPP 5.1 requires an organisation to have a written policy about its management of personal information, which must be made available on request. OVIC encourages organisations to publish this policy.

IPP 5.2 requires an organisation to tell people, if they ask, about the sorts of personal information the organisation holds, and how it handles that information.

5.1 IPP 5 requires organisations to have a privacy policy. Privacy policies should be clear and accessible. The primary purpose of the policy is to tell the public how the organisation handles personal information. A clear and accurate privacy policy supports a positive, trusting relationship between the organisation and members of the public. The drafting and ongoing review of privacy policies is part of an organisation's privacy governance.

5.2 Organisations must also tell people, if they ask, about the information the organisation holds and how it is handled. This requires an organisation to establish procedures to respond to queries about its personal information handling practices, for example, by appointing a privacy officer and publishing their contact details.

IPP 5.1: Written policy on management of personal information

5.3 IPP 5.1 states:

> An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.4 Victorian public sector organisations and contractors bound by the PDP Act must have a privacy policy. An organisation should periodically review its privacy policy, especially where it has been given new functions or has undergone a restructure. OVIC recommends organisations schedule a regular review of their privacy policy at least once a year. The periodic review of a privacy policy should ideally be subject to executive sign-off, to ensure executive members of staff have oversight of the organisation's privacy practices.[1]

5.5 It is good practice (and consistent obligations under the *Public Records Act 1973* (Vic) (**Public Records Act**) to keep full and accurate records) to include a date and version reference on a privacy policy.

[1] There is no explicit requirement to review a privacy policy in the PDP Act. In considering how to conduct a review, organisations may wish to consider the approaches outlined in more codified privacy regimes. For example, the Australian Government Agencies Privacy Code requires agencies to develop a privacy management plan, and review it annually. The EU General Data Protection Regulation requires that Data Protection Officers appointed under the Regulation 'directly report to the highest management level of the controller or the processor' under Article 38(3). Victorian public sector organisations can use the drafting and periodic review of privacy policies as an opportunity to demonstrate good privacy governance, and to ensure they are meeting their IPP 5 obligations.

This helps establish which policy was in effect at any given time and may be relevant to assessing whether an organisation took reasonable steps at the time of an alleged breach or complaint, or what a person might have reasonably expected from the organisation at that time.

5.6 Preparing to write a privacy policy involves examining the way personal information is gathered and flows through an organisation. The key to an effective privacy policy is appropriately tailored to what the organisation does with personal information, what it needs to do, what it properly can do. An effective privacy policy also ensures the organisation actually complies with its privacy policy. A privacy policy should not be a reproduction of the IPPs.

5.7 In drafting a privacy policy, there is no one-size-fits-all approach. It is insufficient for an organisation to copy another organisation's policy. Organisations may consult the work of others and take the best from good privacy policies, but they should first and foremost consider how their own privacy policies will operate.

5.8 Large organisations should consider whether they should have more than one privacy policy to cover, for example, the activities of individual business units which have distinct functions. It may be appropriate for an organisation to have different policies to cover different types of information or information handling practices. A separate website policy, email monitoring policy or a social media policy are examples. An organisation may wish to consolidate their obligations under the PDP Act and *Health Records Act 2001* (Vic), in relation to personal and health information respectively, into a single document or set of documents.[2]

Case Study 5A: An organisation should ensure its actual practice accords with its privacy policy

A person ('the complainant') registered members of their family for a program, which was being delivered by a contracted service provider ('the company') to an organisation. The company was part of a large conglomerate of commercial businesses offering a wide range of services.

The complainant was concerned by the company's privacy policy. The policy suggested the company over-collected the personal information of program participants from a broad range of parties.

The policy also appeared to state the organisation retained personal information indefinitely: it advised it kept customers' personal information (for purposes such as market research), even after they no longer used the program's services.

Furthermore, the policy indicated personal information would be disclosed to its related companies, a range of service providers and business partners outside Victoria, in a way contrary to the requirements of the PDP Act.

When the complainant contacted the company's privacy officer to express their concerns, they received no response.

The complainant made a formal complaint to OVIC. The company conceded its policy had been drafted by an external consultant. The policy reflected the information handling

[2] More information on how to draft privacy policies is on OVIC's website.

practices of the larger conglomerate rather than the company concerned. The company agreed to revise its privacy policy so it more accurately expressed its actual information handling practices.

Publishing the privacy policy

5.9 There is no specific requirement under IPP 5.1 to publish the privacy policy – only to make it available on request to anyone who asks. Nonetheless, an organisation may find it convenient and cost effective to publish its policy on its website. Publishing privacy policies for members of the public to easily access also increases transparency of government.

5.10 As a matter of good practice, OVIC suggests all organisations make their privacy policies publicly available online. Other options include:

- sending a privacy policy with written correspondence to individuals when they first transact with, or become a client of, an organisation;
- referring to the privacy policy with annual notices such as re-registration forms; and,
- having a copy of a privacy policy available at an organisation's enquiries desk or counter.

Writing a privacy policy

5.11 Organisations should ensure that privacy policies use clear and accessible language. As a matter of best practice, a privacy policy should include at least:

- the identity of the organisation and how to contact it;
- the organisation's main functions and the types of personal information the organisation generally collects and holds to fulfil those functions;
- how personal information is used by the organisation, and to whom it is routinely disclosed;
- whether collection of personal information is compulsory or optional (including a reference to any legislation which authorises the collection, use or disclosure of the information, such as the *Local Government Act 1989*);
- how personal information is secured and access to it managed;
- how privacy is protected if the information is transferred or stored outside Victoria;
- the organisation's privacy officer or unit and information about how to make a complaint or seek further information;
- whether the organisation uses CSPs, and which organisation is responsible for compliance (receiving complaints and answering questions in relation to different services); and,
- the date and version reference of the policy.

5.12 Organisations should ensure privacy policies are drafted to suit different audiences. For example, where an organisation often deals with the personal information of children, age-appropriate language should be used to ensure children can understand the privacy policy. Individuals reading a privacy policy should be able to easily understand how their personal information may be handled, to allow them to exercise their information rights.

5.13 There is no single way to draft a privacy policy. Organisations should consider the best way to draft and publish their privacy policy according to the types of personal information they most commonly handle and for which purposes.

5.14 When an organisation is drafting or reviewing their privacy policy, it is important to ensure the audience and purpose is carefully considered. Policies drafted primarily with an organisation's compliance with the PDP Act in mind, and which are approached with a 'set and forget' mentality, often result in little meaningful information being provided to individuals. This prevents individuals from making informed choices when interacting with the organisation.

5.15 OVIC's IPP 5 Self Assessment Tool may help organisations draft and review their privacy policy or privacy policies by prompting organisations to consider the different aspects of a good policy, including findability, version control, and important content to include.[3]

5.16 It may be appropriate for an organisation to take a layered approach to its privacy policies. For example, a brief outline of the organisation's privacy policy may be provided on a form, sign or poster, referring to the full privacy policy contained on the organisation's website or in a brochure. This alerts individuals to the existence of a privacy policy and allows them to seek out further information if they wish.

Availability of privacy policies

5.17 Privacy policies should be readily available to staff within an organisation so that a prompt response can be given to a request from a member of the public that the privacy policy be made available.

Case Study 5B: Failure to provide privacy policy despite repeated request[4]

A woman was concerned about being filmed by a television cameraman while she was travelling on public transport. The filming was being carried out by a media organisation with the consent of a contractor to a government department.

On returning home, the woman contacted the contractor and asked the customer service officer to confirm she had not been filmed and to provide her with a copy of the contractor's privacy policy. The officer said she would take some time to confirm the woman's request about not being filmed and agreed to send out the privacy policy. The woman did not receive the policy. Several days later, the woman saw her image on a television current affairs program.

The woman telephoned the contractor twice more. Each time, she asked for the privacy policy to be sent to her. Each time, she was told it would be sent out, but never received it. The woman then complained to the Commissioner.

IPP 5 requires an organisation to make its privacy policy available to anyone who asks for it. Here, the organisation had failed to make the privacy policy available to her on her request. The complaint was successfully conciliated with the contractor giving a written assurance it would publish a reminder to all staff in an internal newsletter about the importance of privacy laws and ensuring any requests for copies of its privacy policy would be promptly met.

[3] The IPP 5 Self Assessment Tool was developed following OVIC's Examination of Local Government Privacy Policies. The full report is accessible here.

[4] *Complainant G v Department* [2004] VPrivCmr 1.

Timeframe to provide the privacy policy

5.18 IPP 5.1 requires an organisation make its privacy policy available 'to anyone who asks for it'.

5.19 Although IPP 5.1 does not specify a timeframe, if an organisation takes an unduly long time to provide its privacy policy in response to a request, it will not have provided the policy 'on request', which may amount to a breach of IPP 5.

5.20 The requirement to provide a copy of a privacy policy to an individual 'on request' necessarily implies the request must be completed in a reasonable period. Due to advances in telecommunications technologies and changing community expectations, this period may be shorter than it was when hard copy policies were sent by post. In most cases, requests should be able to be responded to very quickly by email or by reference to an online copy of a policy.

5.21 As a matter of best practice, organisations should ensure their privacy policies are either publicly available (for example, on their website) or can be provided promptly in response to a request.

IPP 5.2: Responding to requests about the sort of information held and how it is used

5.22 IPP 5.2 states:

> On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

5.23 IPP 5.2 requires organisations to take reasonable steps, when asked, to let people know what kind of personal information the organisation collects and how it uses it. Unlike IPP 5.1, IPP 5.2 does not expressly require an organisation to document the sorts of personal information it collects and handles.

5.24 IPP 5.2 does not require an organisation to inform individuals about what information is specifically held about them. Requests for access to personal information are governed by IPP 6 and the *Freedom of Information Act 1982* (Vic) (**FOI Act**).

5.25 For IPP 5.1, it is sufficient to give information about the sort of information that is held, its purposes, and how it is collected, held, used and disclosed. IPP 5.2 should be seen as a requirement for a further, more detailed level of information beyond the minimum required in an IPP 5.1 privacy policy.

5.26 An organisation may find it more efficient to meet the requirements of IPP 5.1 and anticipate common queries under IPP 5.2 in the same document. An organisation's published Information Asset Register[5] (**IAR**) may meet some or all of the requirements of IPP 5.2. It may also be useful for an organisation to refer to their IAR when drafting or reviewing their privacy policy, to gain a complete picture of the types of information they hold.

5.27 However, if an organisation receives a request for information that is not answered by its published information, the organisation is required to take reasonable steps to respond. For example, an organisation's privacy policy may not explicitly discuss its practice of taking and using photographs,

[5] See, the VPDSF Information Security Management Collection guidance for more information about Information Asset Registers.

monitoring email, or recording telephone conversations. If an individual subsequently asks for information about these practices, the organisation should be able to provide a tailored response.

5.28 In practice, staff will need to help people understand how the generic descriptions in an organisation's privacy policy apply to the individual's own personal information. The privacy policy and any other information sought by an individual may be that individual's starting point in deciding whether to make an access request under the FOI Act or IPP 6 (Access and Correction).

Relationship between IPP 5 and other information handling obligations

5.29 A privacy policy is a statement about how an organisation manages the personal information it collects. It is a general, non-exhaustive statement about how personal information flows through an organisation. This is different to a collection notice, required by IPP 1.3. A collection notice addresses a specific collection practice of an organisation (such as collecting personal information on a council planning application form, or for a job application).

5.30 A privacy policy can help people decide whether to make an application for access to information held by an organisation under IPP 6 (Access and Correction) or the FOI Act. People must know what type of information is generally held by an organisation so they can specifically ask for access to that information.

5.31 There are similarities in the obligations under IPP 5 (Openness) and Part II of the FOI Act. Part II of the FOI Act requires agencies to publish various statements, including a statement of the categories of documents in the possession of an agency,[6] which are appropriate for assisting the public to effectively exercise their rights under the FOI Act.[7] These requirements may also assist agencies meet their obligations under the Public Records Act, to keep full and accurate records.[8]

Frequently asked questions (FAQs)

What should a privacy policy contain?

5.32 A privacy policy must explain an organisation's information handling practices. It will usually discuss the IPPs but should not simply reproduce them. It should be concise, targeted to the general public, written in plain English and easy to read. Privacy policies should also be tailored to reflect the operations and functions of the specific Victorian government organisation, be that a department, agency or service provider.

5.33 A privacy policy should generally include at least:

- the identity of the organisation and how to contact it;
- the organisation's main functions and the sorts of personal information the organisation generally collects and holds to fulfil those functions;
- how personal information is used by the organisation, and to whom it is routinely disclosed;
- whether collection of personal information is compulsory or optional (referring to any legislation which authorises the collection, use or disclosure of the information, such as the

[6] Under s 7(1)(a)(ii) of the FOI Act.

[7] Under s 7(2) of the FOI Act.

[8] See s 13 of the *Public Records Act 1973* (Vic).

Local Government Act 1989);

- how personal information is secured and access to it managed;
- how privacy is protected if the information is transferred or stored outside Victoria;
- the organisation's privacy officer or unit and information about how to make a complaint or seek further information;
- if the organisation uses CSPs, which organisation is responsible for compliance (receiving complaints and answering questions in relation to different services); and,
- the date and version reference of the policy.

What is the difference between a privacy policy, collection notice and consent form?

5.34 **Privacy policies** explain an organisation's information management practices in a broad sense. They explain how the organisation manages personal information.

5.35 **Collection notices** outline the information handling practices of organisations for a specific purpose and are a requirement of IPP 1.3. See also the discussion: The difference between privacy policies and collection notices.

5.36 **Consent forms** specify a particular reason for the collection, use or disclosure of a personal information, for the purpose of seeking an individual's agreement to a particular information handling practice.

How often should an organisation review its privacy policy?

5.37 An organisation should review its privacy policy when it has been given new functions, has undergone a restructure, has significantly changed its practices, or if there has been an amendment to any relevant legislation. If an organisation begins to collect more information or uses or discloses the information in new ways, for example, where the introduction of a new technology has changed how an organisation handles personal information, this should be immediately reflected in the organisation's privacy policy.[9]

5.38 As a matter of best practice, OVIC suggests organisations schedule a review of their privacy policies at least once every 12 months.

What if an organisation provides different types of services – do they need to have more than one privacy policy?

5.39 If an organisation offers a range of services, it can consider having several privacy policies. While a privacy policy is not as specific as a collection notice, attempting to draft a one-size-fits-all policy can reduce its clarity. A balance needs to be struck between being making the policy accessible and easy to understand, but not misrepresenting the organisation's activities to the individual service user.

[9] See OVIC's website for more information about privacy policies and collection notices.

Should an organisation cover health information in their privacy policy?

5.40 Some organisations collect and handle health information in addition to other personal information. The *Health Records Act 2001* (Vic) contains Health Privacy Principles that are similar to the IPPs in the PDP Act. Organisations may prefer to develop one privacy policy that addresses the principles under both Acts.

5.41 For more information about health information and privacy, contact the Health Complaints Commissioner.

Who should draft a privacy policy?

5.42 An organisation's privacy officer should be involved in the drafting of a privacy policy. The role of a privacy officer involves ensuring the organisation upholds their obligations under the IPPs. The privacy officer will therefore be well placed to coordinate the development of the privacy policy.

5.43 If an organisation decides to outsource this task, they should ensure there is adequate consultation with relevant staff within the organisation, including the privacy officer. Otherwise, there is a risk that the privacy policy will be drafted by someone who does not have a deep understanding of the organisation's information handling practices. An organisation's privacy policy must adequately represent how the organisation will actually manage an individual's personal information (see Case Study 5A, above).

5.44 It is also important to involve communications professionals in the drafting process, to help ensure the language and content of the privacy policy is clear and easy to understand. An organisation's ICT or information security professionals may also be able to assist in outlining the types of protections the organisation has in place to secure personal information.

5.45 Privacy policies should be user friendly and drafted with members of the public as the intended audience in mind.

How can an organisation effectively distribute their privacy policy?

5.46 To meet their IPP 5 obligations, organisations should make their privacy policy readily available for anyone on request. In general, organisations should publish the latest version of their privacy policy or policies on their website.

5.47 As a matter of best practice, individuals should not have to get in touch with the organisation to request a copy of their privacy policy, it should be readily available.

What if an organisation collects personal information from children – how can they draft a privacy policy for a young audience?

5.48 Any communications drafted for children should be age-appropriate, using clear, easy to understand language. Individuals reading a privacy policy should be able to easily ascertain how their personal information may be handled, in order to allow them to exercise their information rights.

Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

Version control table

Version	Description	Date published
IPP 5 (Openness) 2019.B	Edits following consultation.	14 November 2019
IPP 5: Openness 2019.A	Consultation draft.	28 February 2019
IPP 5: Openness (2011)	2011 pdf version.	2011