Commissioner for Privacy and Data Protection

FAQs

Local Councils and Privacy: Frequently Asked Questions

Table of Contents

Introduction

Local councils collect a vast amount of personal information about individuals in their daily functions, from information about ratepayers and pet owners, to details of complaints made to the council. This Frequently Asked Questions (FAQs) document is designed to address some of the most common enquiries Victorian local councils have in relation to their privacy obligations under the *Privacy and Data Protection Act 2014* (PDPA), and provide links to more detailed guidance on specific topics published by the Office of the Commissioner for Privacy and Data Protection (CPDP).

Local councils and the *Privacy and Data Protection Act 2014*

1. **What obligations do local councils have to comply with the *Privacy and Data Protection Act 2014*?**

   In Victoria, local councils are required to comply with Part 3 of the PDPA – Information Privacy – which provides for the responsible handling of ***personal information*** by Victorian public sector organisations.[1] Where a local council collects, holds, uses or discloses personal information, it must comply with the 10 Information Privacy Principles (IPPs) listed in Schedule 1 of the PDPA. The IPPs set out the minimum standards for how the Victorian public sector should handle personal information, from the time it is first collected until it is disposed of when no longer required. Some of the matters that organisations must consider include the types of information they are permitted to collect, how they use and share that information, how they protect it, and for how long they are able to retain it.

   While Part 4 of the PDPA – Protective Data Security – does not *expressly* apply to local councils,[2] councils are required to take 'reasonable steps' to protect personal information from misuse, loss, unauthorised access, modification and disclosure under IPP 4.1. It is the position of CPDP that the Victorian Protective Data Security Standards (VPDSS), issued under Part 4 of the PDPA, amount to 'reasonable steps' for the purposes of IPP 4.1. Consequently, Victorian local councils incur an indirect obligation to comply with the data security requirements set out in Part 4 of the PDPA. Further guidance on this topic is available in the *Guidelines to protecting the security of personal information: 'Reasonable steps' under Information Privacy Principle 4.1.*

2. **Who within a local council is required to comply with the PDPA?**

   Part 3 of the PDPA expressly applies to both local councils as organisations,[3] and elected councillors in their capacity as a person holding office.[4] This means that all employees of a local council, as well as individual councillors representing their constituents, will need to handle personal information in accordance with the IPPs. Part 3 of the PDPA will also apply to branches of local councils, such as community libraries and childcare centres. External contractors that have been engaged to provide a

[1] Personal information is defined in s 3 of the *Privacy and Data Protection Act 2014* as '*information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the* ***Health Records Act 2001*** *applies.*'

[2] See, *Privacy and Data Protection Act 2014*, s 84(2)(a).

[3] Under s 13(1)(d) of the *Privacy and Data Protection Act 2014*.

[4] As councillors hold office under the *Local Government Act 1989*, they are bound to comply with the *Privacy and Data Protection Act 2014* under s 13(1)(g) of the PDPA.

service or function on behalf of a local council may also have obligations under the PDPA. Please see question 10 below for further information on outsourcing.

Managing the collection of personal information

3. How should local councils provide collection notices, particularly where information is collected indirectly about individuals?

A local council must provide notice of collection to individuals each time personal information is collected, to make individuals aware of why their personal information is being collected and how it will be used. IPP 1.3 stipulates what a collection notice needs to contain, but organisations are able to provide that notice in whichever way they see fit. The way in which a collection notice is provided will likely depend on how the information is collected. For example, collection notices could be printed on forms that individuals are asked to fill in, or may be provided orally when a council officer collects personal information over the telephone.

As local councils will likely collect personal information from individuals for a number of their functions and activities, different collection notices may need to be provided for each of the council's separate functions. For instance, the collection notice that accompanies an online payment system will be different from the one provided by a library to new members when they join, as different types of personal information will be collected for these council functions, and for different purposes. Please see our guidance on *Collection notices* for further information on drafting collection notices.

When personal information is collected about an individual indirectly, such as where the information is provided by a third party, IPP 1.5 states that reasonable steps must be taken to ensure that the individual is made aware of the collection. What constitutes 'reasonable steps' will depend on a number of factors, and in deciding on the steps to take, local councils should consider factors such as the nature of the information in question, how the council will use the information, and whether the council would in fact need to collect *additional* personal information in order to make contact with the individual to provide them with a collection notice. In some cases, a local council may decide that it is reasonable to take *no* steps to notify an individual of the collection.

An example of where it may be appropriate for a local council to take **no steps** under IPP 1.5 is where **unsolicited information** is received – that is, where the council did not specifically request or require the information. Unsolicited information that is personal information will still be subject to the IPPs, as the PDPA does not differentiate between unsolicited information and personal information that is intentionally collected (as is the case in other jurisdictions). Yet if a local council receives unsolicited information that is not necessary for its functions – and it has no intention to use the information – the council may decide that it is reasonable in the circumstances not to notify the individual of the collection, and simply store the information in accordance with the *Public Records Act 1973.*

4. **Can a local council publish documents that contain personal information, such as submissions, objections, permit applications, gift registers and meeting minutes?**

   Local councils are required by law to publish certain documents such as local laws, current budgets and annual reports.[5] A local council may also publish documents such as meeting minutes, planning permit applications, gift registers, and submissions or objections on particular matters. Where a local council intends to publish documents such as these that contain personal information, this must be done in accordance with the PDPA and any other legislation that specifically requires or permits their publication, such as the *Local Government Act 1989*.

   As such, councils should ensure that members of the public are notified of this intention, through the provision of a collection notice in accordance with IPP 1.3 (see above). For example, when seeking submissions to a public consultation, councils should clearly communicate to individuals their intention to publish the documents, making them publicly available. Collection notices should be consistent with the council's privacy policy.

   Where possible, individuals should also be given the opportunity to remain anonymous (IPP 8); if there is no need for the individual to be identifiable, their personal information should not be published. For instance, when publishing gift registers it may not be necessary to identify council officers by name – listing their position may be sufficient. In general, a council should exercise caution when publishing any documents containing personal information and consider whether there is a need to publish personal information at all.

5. **How should local councils manage their use of closed-circuit television (CCTV)?**

   A number of key privacy principles will apply to local councils when using and administering closed-circuit television (CCTV). CCTV cameras are capable of capturing personal information such as images that identify individuals, and in some cases audio. As such, local councils are obliged to ensure that any footage that captures personal information is handled in accordance with the IPPs. Similarly, photographs that contain images of identifiable individuals will attract the same privacy obligations, such as when a parking inspector who takes a photograph of a vehicle also happens to capture individuals in the background.

   To ensure compliance with the IPPs, local councils must first identify a legitimate purpose for the use of CCTV and be able to demonstrate why it is necessary for their functions. Council staff and community members that will be captured must be notified when CCTV cameras are in operation, and the purpose of their use.[6] Local councils should also observe IPP 4 in relation to data security, to ensure that personal information captured by CCTV is stored appropriately, and that only those who are authorised to access the footage are able to do so.

   Before implementing a surveillance program, local councils should undertake an assessment of the potential privacy risks that may arise during the program, by undertaking a privacy impact assessment

[5] Under s 82A of the *Local Government Act 1989*.

[6] More information about the form and location in which notice should be provided can be found in our *Guidelines to surveillance and privacy in the Victorian public sector*.

(PIA). Victoria Police should also be engaged early in the planning stage, as there may be implications if criminal activity is captured. Local councils can refer to the guidance CPDP has published on surveillance, in the *Guidelines to surveillance and privacy in the Victorian public sector* for further information.

6. **When and how should a local council destroy documents containing personal information?**

   When a local council no longer has a need for personal information it holds, steps should be taken to destroy or de-identify the personal information in accordance with IPP 4.2. Retaining personal information after its purpose has lapsed can pose a significant security risk. In fulfilling these obligations under IPP 4.2, local councils should ensure that the personal information is disposed of securely.

   It is important to note that the requirements of IPP 4.2 should be balanced with a local council's obligations under the *Public Records Act 1973* (PRA). Local councils may have specific recordkeeping requirements according to a Retention and Disposal Authority (RDA) stipulating for how long public records must be retained. Where a local council has archived information in accordance with the PRA, this requirement will override a council's obligations under IPP 4.2 as the PRA will determine when it is appropriate to retain or dispose any personal information.[7] For information regarding specific recordkeeping requirements, local councils can contact the Public Records Office of Victoria.

Using and disclosing information under the *Privacy and Data Protection Act 2014*

7. **Can a local council disclose information about an individual to a third party, for example, when investigating a complaint involving neighbours?**

   Only in limited circumstances. IPP 2.1 stipulates that an organisation may only use and disclose personal information for the primary purpose for which it was collected or for a reasonably expected 'secondary purpose' that is related to the primary purpose.[8] However, there are a number of exceptions under IPP 2.1.[9] For example, when responding to a complaint alleging unlawful activity, a local council may be able to rely on IPP 2.1(e) to disclose an individual's personal information to the relevant law enforcement organisation or regulatory authority, provided the council has reason to suspect that unlawful activity has in fact been engaged in. Where a local council receives a complaint from a member of the community concerning the conduct of their neighbour, for example, which involves unlawful activity, IPP 2.1(e) would allow the council to disclose the personal information it received at the time of the complaint, when reporting the matter to police.

   IPP 2.1(g) also expressly authorises organisations to assist police and other law enforcement agencies by providing information relevant to their criminal investigations and law enforcement functions.

[7] As the PDPA is default legislation, setting out a minimum set of standards that local councils must adhere to, IPP 4.2 will apply in cases where other legislation (by which a local council is bound) is silent on recordkeeping.

[8] If the personal information is 'sensitive information' (meaning it relates to certain characteristics specified in the PDPA such as race, political opinion, sexual preference or criminal record) then the secondary purpose must be '*directly* related' to the primary purpose.

[9] See IPP 2.1(a)–(h) for a full list.

Where there is no clear authority to disclose an individual's personal information, it is best to seek the individual's consent before sharing the information.

8. **How should a local council handle requests for access to personal information by third parties?**

   The usual procedure for accessing and correcting documents in the public sector is under the *Freedom of Information Act 1982* (FOI Act). If a third party requests access to any information held by a local council, the FOI Act will apply to provide rights of access. However, the FOI Act may not apply to contracted service providers (CSPs) of local councils. If information held by a CSP is not covered by the FOI Act, rights of access and correction of information are provided by IPP 6, as IPP 6 *only* applies to organisations that are not covered by the FOI Act. If IPP 6 applies, the requested personal information must be provided to the individual unless one of the exceptions under IPP 6.1 is relevant.

   Where a local council receives a request for access to personal information by a law enforcement agency, such as Victoria Police, IPP 2.1(g) will usually permit disclosure (see question 7, above). However, councils should still consider each request on a case by case basis, and make sure that they are satisfied that they are legitimate.

9. **If a local council receives contact details from an individual for one purpose, can those details be subsequently used for another purpose?**

   Only if the secondary purpose relates to the primary purpose for collection, and the individual would *reasonably expect* their contact details to be used for the secondary purpose, under IPP 2.1. What is a reasonably expected secondary purpose will depend on the context. For example, if a local council collects an individual's contact details for the purpose of registering their dog and subsequently uses those contact details to alert the individual of upcoming works to the local dog park, this would likely be considered a related secondary purpose that an individual would reasonably expect for the use of the contact details.

   Councils should also take into account any relevant exceptions that would allow the subsequent use or disclosure of the information under IPP 2.1, such as where there is a serious threat to life under IPP 2.1(d)(i) or where the use and disclosure is required or authorised by law under IPP 2.1(f), for example.[10] Where a local council can anticipate using an individual's contact details for secondary purposes, it is important for the council to ensure that proposed subsequent uses of the information are detailed in collection notices (see question 3, above) and that the use of the contact details or information is consistent with the council's privacy policy.

   If a particular use or disclosure is not otherwise permitted under IPP 2.1, councils can always seek individuals' explicit consent under IPP 2.1(b). It is important to note, however, that simply providing individuals with notice of a new use or disclosure and the opportunity to opt out will not ordinarily be sufficient to say that they have consented to that new use or disclosure.

[10] See IPP 2.1 in Schedule 1 of the *Privacy and Data Protection Act 2014* for a full list of the exceptions under IPP 2.1.

Managing privacy risks

10. How should a local council manage its privacy obligations when outsourcing its activities to a contracted service provider? Which party remains liable for privacy?

In general, a local council will retain its privacy obligations under the PDPA in an outsourcing arrangement, not the CSP.[11] When a local council engages in an outsourcing arrangement with a CSP, such as a community housing provider, the local council by default will be responsible for the CSP's compliance with the IPPs, within the scope of the arrangement.

However, local councils can pass on their privacy obligations to the CSP — that is, contract out of their obligations under Part 3 of the PDPA — by expressly including provisions to this effect in the contract.[12] This will mean that the CSP will be responsible for protecting the personal information it holds and may be liable in the event of a privacy breach. However, even when a CSP has assumed liability for privacy breaches, the council remains ultimately responsible for ensuring that individuals' privacy is protected, even in relation to the outsourced services. This means that councils should ensure that outsourcing contracts are set up in such a way that they do not decrease privacy protections. For example, when engaging a CSP, local councils should ensure that they are choosing a provider that has the resources and expertise to adhere to the IPPs in the same way that a council is required to.

If a council has **not** passed on its privacy obligations to a CSP via a contract, the council will remain responsible for ensuring the personal information held by the CSP is adequately protected. In these cases, councils should establish protocols with the CSP upfront, so both parties are clear on how compliance with the IPPs will be achieved. For example, if an individual requests access to information that the CSP holds about them, the council will be responsible for ensuring compliance with IPP 6 and may need to work with the CSP in order to satisfy the access request.

CPDP has published *Guidelines for outsourcing in the Victorian public sector – Checklist* and *Guidelines for outsourcing in the Victorian public sector – Accompanying guide* for further information.

11. How should local councils develop employee awareness of privacy risks?

Privacy and data security protections are most effective when they form part of the culture of an organisation. Local councils should commit to having a clear privacy policy and implementing good information handling practices that support the privacy policy.[13] CPDP has published guidance on *Drafting a privacy policy*. Appointing a privacy officer will also ensure that privacy risks are considered and accounted for within the day to day operation of local councils. Privacy officers can offer guidance on relevant privacy laws and respond to any privacy concerns individuals may have.

[11] A contracted service provider is a person or body who provides services under a State contract. See s 3 of the *Privacy and Data Protection Act 2014*.

[12] Where a clause of the State contract indicates a strict intention for the CSP to be bound by the PDPA.

[13] In accordance with IPP 5, which requires organisations to clearly set out in a document policies on the way in which they handle personal information. See, IPP 5, Schedule 1, *Privacy and Data Protection Act 2014.*

Local councils are also encouraged to provide ongoing privacy training to all staff. CPDP offers a free online privacy training module which provides an overview of the information privacy obligations that apply to the Victorian public sector. In some cases, council staff may also require project-specific privacy training, particularly when handling personal information in their day to day role.

A good way to establish a positive culture towards privacy obligations is to adopt a *Privacy by Design* approach, where privacy risks are considered and mitigated at the beginning of a project. An effective way for councils to turn their attention to privacy is to conduct a PIA when commencing a new project. This will enable staff working on a specific project to identify privacy risks upfront and remedy any adverse impacts to individuals that may arise.

12. What should a local council do if it suspects a privacy breach?

Regardless of the cause of a suspected privacy breach, CPDP encourages local councils to report the breach to this office, so that our staff can provide guidance on containing and managing the breach. It may also be appropriate to notify the individuals whose personal information was involved in the breach, so that they can take any necessary remedial action. Specific guidance on *Responding to privacy breaches* is available on the CPDP website.

While it can never be guaranteed that a privacy breach will not occur, organisations can take steps to mitigate against them. Implementing and maintaining good information handling policies and practices, updating relevant procedures as required, and offering regular privacy training to staff can minimise the risk of a privacy breach occurring.

Published: July 2017