PRIVACY CONSIDERATIONS FOR LOCAL GOVERNMENT

Local government, or councils, collect, use, and retain vast amounts of information about individuals – from information about ratepayers and pet owners, information relating to planning decisions, details of complaints, and delivering community services such waste management, libraries, recreation centres and kindergartens

This page addresses some of the most common enquiries received by OVIC from councils and provides guidance on improving information management, privacy, and information security practices.

What is personal information?

Personal information is information about an individual who is identified or whose identity is reasonably ascertainable. For further information, see OVIC's guidance on what constitutes personal information.

Local councils are required to handle personal information in accordance with the 10 Information Privacy Principles (**IPPs**) set out in the *Privacy and Data Protection Act 2014* (**PDP Act**).

Collecting, using, and disclosing personal information in local government

What are councils obligations when collecting personal information?

The PDP Act requires councils to tell individuals why they are collecting personal information and how the information will be used. This is usually done via a collection notice, however, can be achieved by any method that conveys the required information to the individual providing personal information.

Notice can be given in different ways depending on the circumstances in which councils collect the information. For example, notice can be given via an online form, a telephone script, or a sign at an event. As councils collect personal information for varied functions, different collection notices may need to be provided for each separate function. For further information, see OVIC's guidance on collection notices.

What is the difference between a collection notice and consent?

Collection notices and consent are different and have distinct requirements. Collection notices outline a council's information handling practices for a specific purpose or activity, while consent relates to an individual expressly permitting an organisation to collect, use, and disclose their personal information. Consent is not always required; however, it is one method by which personal information can be collected. Consent is discussed further below.

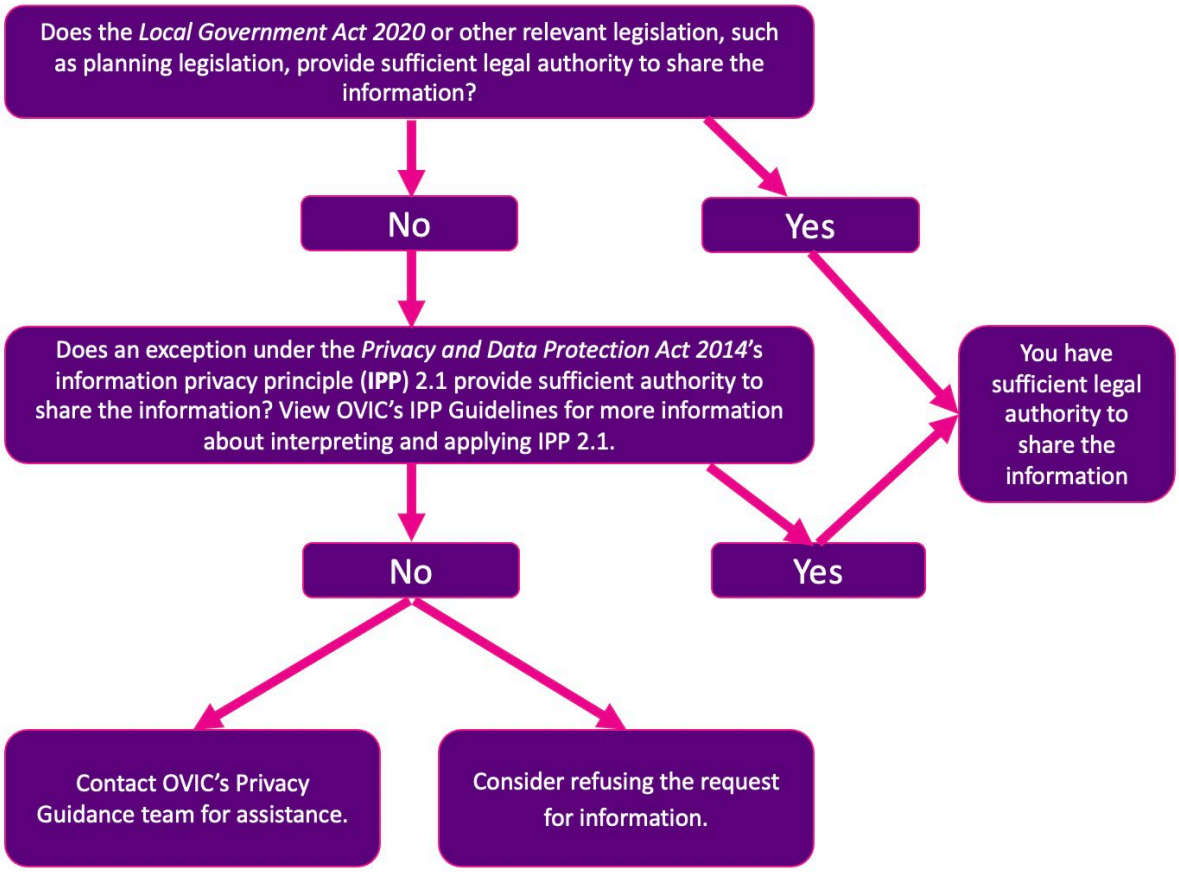
Sharing personal information

Can councils share personal information with other Victorian public sector organisations?

Councils may receive requests for personal information from Victorian public service (**VPS**) organisations such as, Victoria Police, a water authority, or a department.

For example, an Environment Protection Authority (**EPA**) Officer may request that a council share a ratepayer's personal information to assist in an illegal dumping investigation.

To decide whether to share the information, a council should consider the following:



Can a council formalise an information sharing arrangement with a VPS organisation?

Depending on the nature of the information sharing between a council and a VPS organisation, it may be appropriate to prepare an information sharing agreement (**ISA**) to facilitate effective and responsible sharing. Amongst other matters, an ISA sets out the purpose for sharing the information, the type of information to be shared and the duration the information will be shared.

It is important to note that an ISA does not permit the sharing of personal information for purposes not already permitted by legislation or the IPPs. An ISA merely formalises the information sharing arrangements. For further information, see OVIC's guidance on ISAs.

Can councils share personal information with individuals, such as ratepayers?

Councils may receive requests from ratepayers for the personal information of other ratepayers in various circumstances including to address a dog attack, a fencing complaint, or planning of building protection works. Councils should assess the request comprehensively before deciding whether to share information.

Example

The victim of a dog attack lodges a complaint with their local council. The council contacts the dog's owner, and the owner requests the contact details of the victim, with the stated intention of apologising to the victim. The council needs to determine whether it can share the information requested.

Guided by the decision-making flowchart above, the council takes the following steps:

1. Reviews the *Local Government Act 2020* to identify whether sufficient legal authority to share the information with the victim exists. The council determines there is no such authority.
2. Reviews IPP 2.1 in the PDP Act to determine whether an exception permits the sharing of the victim's personal information.
3. Identifies the consent exception in IPP 2.1(b), which permits the council to share the victim's contact details with the dog's owner provided that the victim specifically consents to this.
4. Reviews the complaint record, which indicates the victim did not consent to having their contact details shared with the dog's owner at the time the complaint was lodged.
5. Contacts the victim to seek consent to share their contact details with the dog's owner. The victim refuses to grant consent.
6. Refuses the dog owner's request to share the victim's personal information.

How can councils gain valid consent to share personal information?

Valid consent can provide councils the legal authority to use and disclose personal information. For consent to be valid and meet the requirements under the PDP Act, it must be voluntary, informed, specific, current, and provided by someone with the capacity to consent.

Consent generally endures for the specified amount of time that individuals have consented to their personal information to be shared. For example, if a council has sought consent to share personal information for a specified purpose, such as a project, consent will endure for the duration of that project. For further information, see OVIC's guidance about consent.

Publishing personal information

Can councils publish planning documents?

Councils are required by law to make certain planning documents publicly available, including permit applications, submissions to amendments and objections to permit applications. This is to ensure transparency and public participation in Victoria's planning system. However, this objective needs to be balanced with privacy.

The *Planning and Environment Act 1987* (**the Act**) allows councils to comply with these requirements by publishing relevant planning documents on their website. However, section 197F of that Act prohibits the disclosure of certain personal information when a planning document is published electronically.

Councils should always make sure they are publishing relevant planning documents in accordance with that Act. More information about the obligations of councils to make planning documents publicly available is provided on the Department of Environment, Land, Water and Planning's (**DELWP**) website.

For privacy queries, councils should contact DELWP. DELWP are best placed to assist councils to understand their obligations in relation to making planning documents publicly available. If after contacting DELWP privacy queries remain, councils should contact OVIC.

What is best practice for publishing other documents on a council's website including recordings of council meetings and meeting minutes?

The *Local Government Act 2020 (**LG Act**)* reflects a stronger focus on public transparency of council decisions. For example, councils must now adopt a public transparency policy to provide transparency for council decision making and outline how council information is to be made publicly available. To fulfil this objective, councils are required to publish certain documents online.

When making personal information publicly available in accordance with a council's public transparency policy, councils and councillors should provide individuals the opportunity to remain anonymous unless expressly required to publish or disclose personal information under the LG Act or other relevant legislation. As far as possible, documents should be published in a privacy-enhancing manner.

Why should councils appoint a privacy officer?

Appointing a privacy officer ensures that privacy risks are considered and accounted for in the day-to-day operation of councils. Their duties include offering in-house guidance on relevant privacy laws, responding to privacy queries and complaints from citizens, and assessing privacy impacts of a council's projects or initiatives. For further information, see OVIC's guidance to help privacy officers perform their functions effectively.

Law enforcement

When is a council a law enforcement agency for purposes of the PDP Act?

Councils engage in law enforcement functions where, for instance, they enforce parking restrictions as council can issue a parking fine for failure to comply with these restrictions.

Councils can use and disclose personal information where the use or disclosure is reasonably necessary for any of five law enforcement purposes set out in IPP 2.1(g). For further information on when council is a law enforcement agency, see OVIC's guidelines to IPP 2.1(f).

Can individuals engage anonymously with councils?

Where it is lawful and practicable, individuals should be allowed to engage anonymously with councils as required by IPP 8. This is intended to maximise individuals' ability to control their personal information. It can also minimise the amount of personal information councils collect thereby minimising the risk of harm caused by a data breach.

Some of the circumstances in which individuals should be allowed to engage anonymously with councils include where councils are seeking feedback on proposed projects, services, or events.

Complaint handling

Whether councils need to collect personal information about complainants will depend on the nature of the complaint. Many complaints can be resolved without collecting a complainant's identifying information. Anonymity can help complainants feel more comfortable discussing their concerns as they are less likely to be afraid of the potential consequences of identifying themselves.

However, in other circumstances, it may not be practicable for the complainant to remain anonymous. Their identity may need to be disclosed so that the party subject to the complaint can fairly respond to the allegations. For further information, see OVIC's resources on anonymity and complaint handling.

Surveys and consultations

In many cases, surveys can be conducted without collecting, using, or disclosing personal information. Councils should take steps to minimise the amount of personal information included in surveys particularly where councils intend to make results of the survey publicly available. If applicable, councils should de-identify surveys before sharing the results. For further information, see OVIC's resources on de-identification.

Security obligations for local councils

Do councils have to comply with the Victorian Protective Data Security Framework?

Part 4 of the PDP Act sets out the information security obligations of Victorian public sector agencies under the Victorian Protective Data Security Framework (**VPDSF**). Councils are expressly exempt from Part 4.

However, where a council performs the functions of other public entities captured by Part 4, such as a Committee of Management (**CoM**) under the *Crown Land Reserves Act 1978* or a cemetery trust, any information relevant to those public functions will be subject to Part 4 of the PDP Act.

If a council cannot separate the information relevant to their functions as a CoM or a cemetery trust from information collected and held by council as part of their day-to-functions, OVIC will consider the entire data-holdings of the council as subject to Part 4 of the PDP Act and the obligations under the VPDSF. For further information, see OVIC's resources about the applicability of the VPDSF.

How can councils improve information security practices?

As well as the obligations under the VPDSF, councils are required to take 'reasonable steps' to protect personal information from misuse, loss, unauthorised access, modification and disclosure under IPP 4.1. For further information, see OVIC's guidance on complying with IPP 4.1.

How should councils respond to data breaches and information security incidents?

Responding to a data breach consists of four key steps: contain, assess, notify, and review. The overriding principle to be followed is harm minimisation—minimising potential harm to affected individuals.

In the event of a data breach, councils should consult OVIC's guidance on responding to a data breach. Councils are strongly encouraged to report any data breaches to OVIC using via the information security and privacy incident notification form. Importantly, councils are required to report information security incidents that meet a certain threshold. For further information, see OVIC's Incident Notification Scheme.