



Office of the Information Commissioner
Queensland



PRIVACY IN LOCAL GOVERNMENT

An introduction to meeting obligations under the *Information Privacy Act 2009 (Qld)*



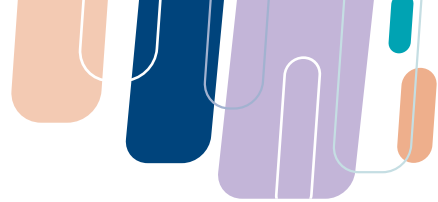


Table of Contents

Introduction	1
Scope	1
Part 1 – Privacy in local government	2
Understanding privacy	2
The privacy obligations that apply	2
Personal information	3
Part 2 – Privacy in practice	5
Establishing a Privacy Policy	6
Providing a Collection Notice	8
Proactive disclosure	14
Personal information holdings	16
Contracted service providers	19
Assessing and managing privacy risks	22
Surveillance technologies	25
Council awareness of privacy issues	30
Privacy program management	35
Staff privacy training and awareness	37
Privacy in multi-service environments	40
Appendix A: Glossary	43
Appendix B: OIC privacy guidance, resources and training	45



Introduction

Providing essential services to the community – such as timely rubbish removal, clean streets, accessible parking, transport and recreation facilities, permits for building work and management of complaints – is one of the primary functions of Queensland local governments (councils). Functions also include employee management and procurement of goods and services. When councils collect personal information in order to attend to these functions, it is important to manage this information in accordance with privacy obligations and community expectations. A failure to do this erodes community trust and may lead to privacy complaints.

Councils may find themselves risking non-compliance when the good decision-making opportunities presented by privacy are perceived as time consuming, expensive or as a potential roadblock to council projects or initiatives.

This resource booklet is broken into two parts.

Part 1 discusses the concept of privacy and provides a brief overview of privacy requirements for Queensland councils.

Part 2 supports Queensland councils to understand and apply the privacy principles. It provides practical guidance for local government situations, tips, and links to resources and guidance on the Office of the Information Commissioner (OIC) website. Part 2 will assist councils to meet their privacy obligations and, ultimately, to make good decisions in relation to the collection and handling of personal information.

For direct links to OIC resources referred to in this booklet, see Appendix B.

Scope

This resource booklet focuses on privacy obligations set out in the *Information Privacy Act 2009* (IP Act).

Councils also have related obligations under other laws such as the *Right to Information Act 2009* (RTI Act) and the *Human Rights Act 2019*. While this resource touches on the application of these laws, it does not provide specific guidance on council obligations under other laws that are related to privacy.

The Office of the Information Commissioner acknowledges Aboriginal and Torres Strait Islander peoples as the First Australians and recognises their culture, history and diversity, and their deep connection to the land, waters and seas of Queensland and the Torres Strait. We acknowledge the traditional custodians of the lands on which we operate and wish to pay our respects to their Elders past, present and emerging.



Part 1 – Privacy in local government

Queensland councils collect and handle significant amounts of personal information. Compliance with the IP Act supports accountable information practices and fosters ongoing engagement and involvement of the community.

Part 1 discusses the concept of privacy and provides a brief overview of privacy requirements for Queensland councils, including:

- understanding privacy
- the privacy principles that apply
- personal information.

Understanding privacy

It is helpful to think about privacy as the **protection of personal information in accordance with the IP Act ... and community expectations.**

Embedding this understanding of privacy in day-to-day practice improves council decisions involving personal information, and helps to build a culture of responsible information practice that staff and the community can rely on. The benefits of, and opportunities for, embedding privacy in council decisions are discussed in Part 2.

The privacy obligations that apply

Queensland councils are bound by the IP Act including the Information Privacy Principles (IPPs), which set obligations for how personal information is managed through its life cycle.¹

Broadly, the IPPs outline obligations about:

- transparency of council's personal information handling practices
- the collection, use and disclosure of personal information
- storage and security of personal information
- the accuracy of personal information
- an individual's right of access to and correction of their own personal information.

The OIC provides further guidance on the IPPs in the [Overview of the Information Privacy Principles](#).

In addition to the IPPs, the IP Act also sets obligations for:

- the transfer of personal information outside of Australia, set out in section 33 of the IP Act
- arrangements with contracted service providers that involve personal information, as required by Chapter 2, Part 4 of the IP Act.



Personal information

Put simply, personal information is **information about a person that identifies them or allows them to be identified.**

Personal information is not limited to name and contact information. It may also include information such as photos or video footage of a person, device details, opinions or preferences, email contents, payment history, salary, physical characteristics or uniquely identifying numbers (such as driver licence number). Personal information does not always have to identify an individual directly but could be combined with other information to allow an individual to be identified.

Personal information is defined in the IP Act as:

Information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Figure 1, Types of Personal Information, provides examples of information that may be considered personal information, either on its own or in combination with other information.

Some types of personal information may be considered sensitive from the perspective of the individual it relates to, such as information about a person's religion, criminal history or sexual preferences. Care should be taken to assess potential levels of sensitivity when collecting and handling personal information.

Some of the types of personal information can overlap. Some examples include:

- Tracking information (e.g. location), spatial information (e.g. drone footage) and services sought (e.g. permit application) may all be elements associated with council building and development approval processes.
- Identifying information (e.g. library card number), personal understanding information (e.g. a person's knowledge and beliefs) and family information (e.g. parent details) may be associated with a children's writing competition run by the council library.

[Download Types of Personal Information Poster \(PDF\)](#)

To support ongoing community engagement and trust, councils should be aware of community perceptions about the sensitivity of personal information and consider whether additional safeguards are needed in the circumstance.² For example, in relation to a disability parking permit, it is likely that an individual would reasonably expect council to collect and handle their medical information (e.g. details of a disability) with additional care.

The OIC provides further guidance about [personal information](#) and [key privacy concepts](#).

² Refer to IPP 4(2), which requires that: 'Protection ... must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.'

Figure 1 – Types of Personal Information

Outer Person

Identifying
Identifies a person – e.g. name, image captured on CCTV, driver licence number, passport number, biometric (faceprint, fingerprint), library card number

Physical
A person’s physical features – e.g. age, DOB, gender, physical features captured by surveillance (e.g. hair type, skin tone, tattoos)

Ethnicity
Describes or reveals a person’s ethnic origins – e.g. nationality, language spoken

Demographic
About a person’s characteristics that are shared with others – e.g. income bracket

Health
About a person’s health – e.g. injury details, TPI pension membership number

Sexual
About a person’s sexual life or identity – e.g. transaction with council

History

Significant events that happened in a person’s life – e.g. Brisbane floods

Finances

Personal Possession
Things a person has owned, rented or borrowed – e.g. house ownership/ rental information, vehicle registration number

Account
About a person’s financial accounts – e.g. credit card and bank information

Credit
About a person’s financial reputation – e.g. payment history

Spending
About a person’s purchases, spending or income – e.g. transactions with council

Service Sought or Supplied

Interactions with council
About a person’s dealings with council – e.g. access to services or benefits (e.g. special transport), permits and applications (e.g. building approval), mandatory payments (e.g. rates payment, dog registration payment), details of disputes and complaints



Tracking

Personal Device
About a personal device or its use – e.g. IP address, use of council webpages

Contact
Details for contacting a person – e.g. email, postal address, phone

Location
About a person’s location – e.g. city/town, device location

Inner Person

Authentication
A person’s authenticating information – e.g. passwords, signature

Opinions
Personal preferences, opinions or interests – e.g. preferred activities, survey opinions, petitioner details, feedback

Personal Understanding
A person’s knowledge or beliefs – e.g. religion, personal account of an event (e.g. animal sighting, reporting graffiti)

Interactions

Communications
A person’s communications – e.g. phone recording, email communication

Social Connections
About a person’s friends or social connections – e.g. social media account name and details

Family
About a person’s family and relationships – e.g. emergency contact, parent details

Public Life
About a person’s public life – e.g. community group membership

Occupation and Education
About a person’s education or career – e.g. work role, work history, blue card number, school and class details

Criminal
About a person’s criminal history – e.g. criminal convictions, infringement details

Spatial Information

Area occupied by a person, their dwelling or their land – e.g. RP/SP data, land surveys, drone footage, residential address

Part 2 – Privacy in practice

Part 2 supports Queensland councils to understand and apply the privacy principles. It provides practical guidance on the following topics.

Establishing a Privacy Policy	6
Providing a Collection Notice	8
Proactive disclosure	14
Personal information holdings	16
Contracted service providers	19
Assessing and managing privacy risks	22
Surveillance technologies	25
Council awareness of privacy issues, including	30
- Privacy complaints	30
- Privacy breaches	34
Privacy program management	35
Staff awareness and training	37
Privacy in multi-service environments	40

How to use Part 2

Each topic in Part 2 of this booklet contains:



Tips



Local government obligations



Practical guidance



More information links to further OIC resources and guidance

Establishing a Privacy Policy

Establishing and implementing a **Privacy Policy** helps councils to be transparent and open with the community about their personal information handling practices. Where council's approach to privacy is easy to find and written in plain language, this elevates community awareness about key matters, such as what personal information council holds, why it collects and uses personal information, and how an individual can seek access to the information council holds about them.



Tips

Drafting a Privacy Policy

1. Write in a clear and concise manner, using plain language. Avoid the use of legal jargon.
2. Correctly reference the IP Act and the Information Privacy Principles.
3. Provide sufficient detail about the types of personal information council holds, and the purposes for using the personal information. Do not just quote IP Act requirements.
4. Seek input from council business areas to ensure a good understanding of personal information needs and handling practices of council.
5. Provide council contact information for access or correction requests, and privacy enquiries or complaints.

Publishing the Privacy Policy

6. Publish the Privacy Policy on the council website and ensure it is easy to locate.
7. Consider making the Privacy Policy available in hard copy (e.g. via a brochure) in public access areas.

Revising the Privacy Policy

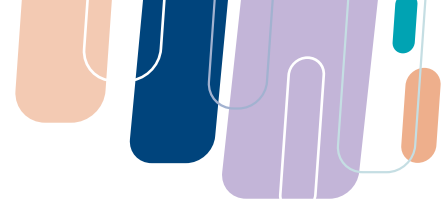
8. Ensure the policy remains up-to-date and accurately reflects the personal information handling practices of council.



Local government obligations

Under IPP 5 of the IP Act, councils must ensure that an individual can find out:

- whether council holds personal information
- the general type of personal information held by council
- the main purposes for which personal information is held
- how an individual can access their own personal information.



Creating and publishing a Privacy Policy (or other documentation such as a brochure, dedicated privacy webpage or a publicly accessible privacy plan) that addresses the above points helps to address IPP 5 requirements and to improve awareness of the community generally.

A Privacy Policy informs community members about the types of personal information that council holds, why it collects and uses that information, and how that information will be handled. Being open with the community about how their information will be collected, used, disclosed and managed increases trust and community engagement.



Practical guidance

Planning a Privacy Policy

A good Privacy Policy requires the person drafting it to have a detailed understanding of how council operates and how council deals with the personal information of its staff and the community.

The person tasked with drafting or revising a Privacy Policy may require input from across council to ensure council operations and personal information handling are properly represented. Consider input from customer service, human resources, local law compliance, maintenance, technology and innovation, governance, information security and the executive team.

Writing a Privacy Policy

When drafting or revising a Privacy Policy, ensure that it:

- is written concisely
- uses language that is easy to understand and avoids 'legalese'
- is clearly labelled (e.g. 'Privacy Policy', 'Privacy Plan', 'Your Privacy and Council')
- is easy to locate on the council website
- is, where practical, available in hard copy in areas of council open to the community (e.g. libraries, customer service centres)
- accurately reflects what council needs personal information for, and explains how council complies with the IPPs and other requirements of the IP Act (not just that it must comply)
- details how an individual can seek access to or correct their own personal information
- details how to ask a question about privacy or make a privacy complaint
- is regularly reviewed to ensure the ongoing accuracy of the document.



More information

- [Access and openness obligations](#)

Providing a Collection Notice

Where practicable, councils are required to take reasonable steps to make people generally aware of certain matters before collecting personal information from them directly (or otherwise as soon as possible after the personal information is collected). This is done by providing a written or verbal 'Collection Notice'. A Collection Notice is sometimes referred to as a 'Privacy Notice', 'Privacy Statement' or 'Privacy Disclaimer'.



Tips

1. Take reasonable steps to provide a Collection Notice when collecting personal information unless an exception applies.
2. Ensure the Collection Notice is specific to each collection circumstance. Do not use the same Collection Notice for every collection conducted by the council.
3. Use plain language that is easy to read and understand.
4. Include all matters required by IPP 2(3):
 - why the information is being collected
 - whether council is authorised or required under law to collect the information
 - council's usual practices for disclosing personal information of that type.
5. Provide the Collection Notice before collection, wherever possible.
6. Remember, a Collection Notice informs a person, it does not ask for their permission. Consent should not be blended with the Collection Notice.
7. For consistency, consider using a template for creating Collection Notices.
8. Consider other forms of notice where personal information is being collected via surveillance or other technologies, such as layered or parallel Collection Notices.



Local government obligations

Under IPP 2, councils must take reasonable steps to make people aware of the following before collecting personal information from them directly (or as soon as practicable after collection):

- the purpose of the collection
- whether the collection is authorised or required under a law, and if so, the law authorising or requiring the collection

- whether the personal information is usually disclosed by council to another entity (i.e. the first entity). A 'usual' disclosure is a disclosure that is highly likely to occur, including as part of a standing arrangement or under a legislative obligation
- whether the personal information is usually disclosed by the first entity to another entity (i.e. the second entity).

Councils make people aware by providing a written or verbal 'Collection Notice'. This method of informing an individual helps to establish their expectations about what council will do with their personal information in a particular circumstance.

Under IPP 2(5), councils are not required to provide a Collection Notice in the context of delivering services in an emergency – for example, when collecting personal information to render urgent assistance during a flood event.³



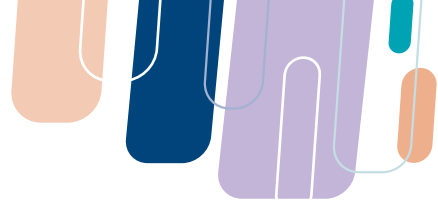
Practical guidance

Some important elements of best practice when providing a Collection Notice are set out below.

A good Collection Notice is:

- 1. not confused with consent** – a Collection Notice informs a person, it does not ask for their permission. If council requires consent from an individual to use or disclose their personal information, this should not be blended with the Collection Notice.
- 2. distinct from the Privacy Policy** – a Privacy Policy sets out general purposes for which council collects personal information, whereas a Collection Notice provides details specific to the circumstance.
- 3. relevant to the circumstance** – councils should not use the same notice across all types of collection.
- 4. provided before collection** – ideally, individuals will be made aware of the matters set out in IPP 2(3) before their personal information is collected. Some ways to do this include:
 - providing a written Collection Notice at the top of an electronic or paper-based collection form
 - giving a verbal Collection Notice before information is collected via phone or in person
 - installing signage that informs an individual before they enter into an area that uses surveillance.

Councils may also benefit from using a **template** to create Collection Notices and should explore whether **other forms of notice** are suitable in particular circumstances (such as where collection occurs via surveillance and other technologies).



Templates

Some written Collection Notice formats to consider.

Written Collection Notice – Template 1

[Council name/department] is collecting personal information from you for the purpose of [specific purpose of collection].

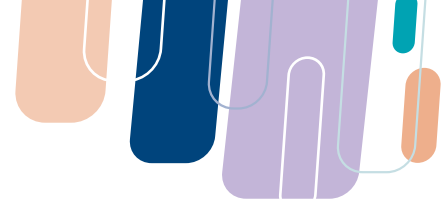
We are collecting your:

- [personal information elements]

The [legislation/bylaw] requires/authorises us to collect this information.

We usually disclose this type of information to [first entity name]. The [first entity name] usually discloses the information to [second entity name]. Council has taken all reasonable steps to ensure that the recipient(s) will only use or disclose your personal information for the purpose that it was provided.

You can read more about how [council name] handles your personal information by visiting our Privacy Policy <insert link>. Questions? Please contact us using [the details on this form/other method].



Written Collection Notice – Template 2

[Council name/department] is collecting personal information from you.



What personal information are we collecting?

We are collecting your [personal information elements].



Why are we collecting your personal information?

We collect this information to [specific purpose of collection].



Legislation that requires/authorises us to collect your information

The [legislation/bylaw] requires/authorises us to collect this information.



Will we share your personal information?

We usually disclose this type of information to [first entity name]. The [first entity name] usually discloses the information to [second entity name]. Council has taken all reasonable steps to ensure that the recipient(s) will only use or disclose your personal information for the purpose that it was provided.

You can read more about how [council name] handles your personal information by visiting our Privacy Policy <insert link>.

Questions? Please contact us using [the details on this form/other method].

In addition to the content included in the templates above, it is also often useful for agencies to express what they will **not** do with personal information. For example, council may include that it will not use an individual’s personal information for any purpose other than the purpose that it was provided for, unless it has a legal authority or requirement to do so.

Other forms of notice

It can be challenging to provide a Collection Notice when personal information is collected by surveillance and other technologies, such as closed circuit television (CCTV) cameras, body worn cameras, parking tech (e.g. sensors, automatic number plate recognition), hop on/hop off transportation (e.g. e-scooters, share bikes) and drones. This is because such collections generally do not involve the use of a form or reliably scripted verbal contact with council officers.

To ensure an individual is generally aware of the collection, and matters regarding the collection, councils may consider providing other forms of notice in these instances including, for example, through the use of icons, QR codes, signage, calling cards (to support a short verbal notice), public advertisements and by publishing information on the council website.

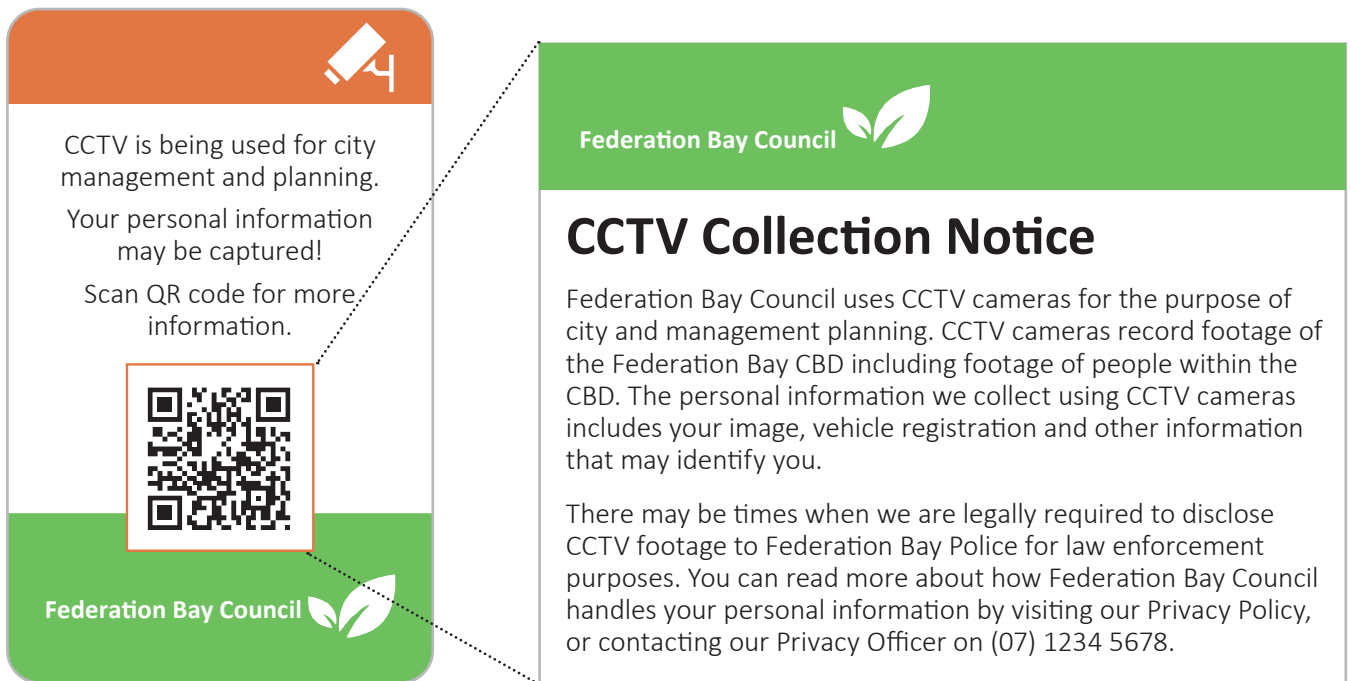
To ensure other forms of notice comply with the requirements of IPP 2, councils may consider using ‘layered’ or ‘parallel’ forms of notice. These concepts are discussed below.

Layered Collection Notice

Layering a Collection Notice involves taking an individual on a privacy discovery, where they learn the top-line information about the collection and can explore the topic in greater depth by continuing a path you have shown them.

Figure 2 is an example of a layered Collection Notice. In this example, a sticker is the first step, which can be affixed to CCTV camera poles or mobile units. The sticker links via a QR code to a dedicated CCTV webpage that provides a longer form Collection Notice.

Figure 2 – Example of a layered Collection Notice



In this case, the layering works as follows:

1. An individual views a sticker placed at eye level on a CCTV camera pole.
2. The individual scans the QR code.
3. The QR code takes them to council's dedicated webpage that explains how it uses CCTV cameras.
4. The dedicated CCTV webpage provides a longer form Collection Notice (such as those in the templates above) and includes a link to council's Privacy Policy.

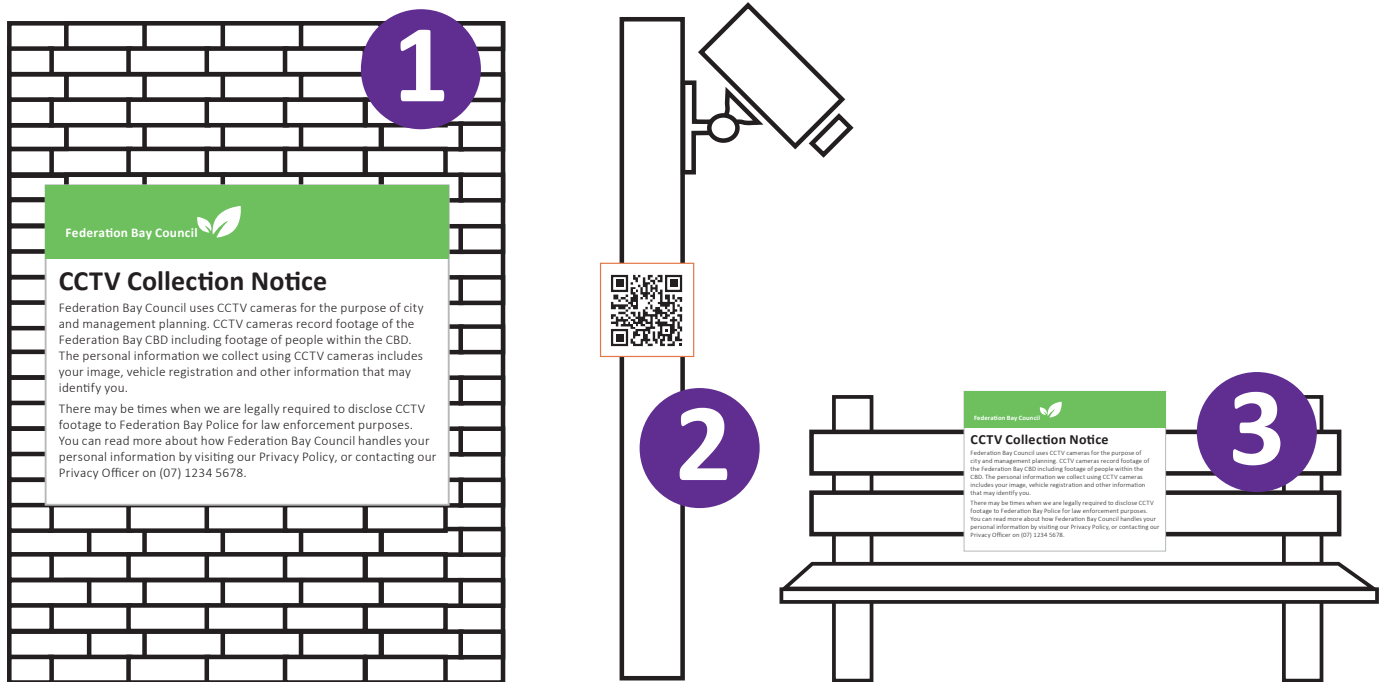


Where QR codes are used, councils should regularly monitor and audit the codes to ensure that they have not been interfered with or altered and continue to correctly link to the appropriate council webpage.

Parallel Collection Notice

A parallel Collection Notice involves providing individuals with the same collection notice (and content) in multiple forms and at different points or locations. Providing a parallel Collection Notice ensures individuals have a number of options available at once to read and understand the collection. See Figure 3.

Figure 3 – Placement of parallel collection notice



In this case, the parallel Collection Notice provides the community with multiple opportunities all at once to be made aware of collection (thereby increasing the opportunity that the notice will be engaged with), including:

1. signage that sets out a full Collection Notice that an individual views when they enter an area that has CCTV cameras
2. a QR code sticker placed on CCTV camera poles that links to a dedicated council webpage that contains a full Collection Notice (i.e. as discussed at 'Layered Collection Notice' above)
3. signage that sets out the full Collection Notice placed on park benches within the area monitored by CCTV



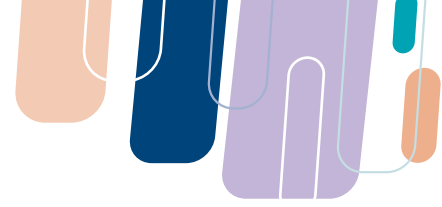
When implementing a parallel Collection Notice approach, councils may also consider:

- providing a form of notice in additional dialects or languages where appropriate
- using eye-catching colours and images to draw the community's attention to the Collection Notice.



More information

- [Collection Notices](#)



Proactive disclosure

Proactive disclosure involves councils deciding to make certain information about their operations available to the public as a matter of course (via the council website or through other means).

Where it is suitable to do so, council should release information proactively in a regular and informal manner, and only refer individuals to formal access to information processes as a last resort.⁴

Councils can benefit from proactively disclosing information to the community about the way they handle personal information. For example, proactive disclosure may:

- reduce formal applications made under the RTI Act for details about council's personal information handling practices
- help individuals seeking access to, or correction of, their own personal information to pinpoint the area of council, or particular information collections, relevant to their request
- ease fear or conjecture in the community about council's use of technologies involving personal information.



Tips

1. Ensure privacy messaging is clear, well-structured and written in plain language.
2. Publish data about the type of information held by council and inform the community that they can apply to access their information.
3. Publish council documents that outline council's privacy strategy, privacy management framework and plans, where available.
4. Publish Privacy Impact Assessment (PIA) summaries.
5. Publish information about council's technology projects that collect or handle personal information, including projects that use AI, IoT, surveillance or facial recognition technologies.



Local government obligations

Local governments have transparency obligations under the IP Act, including requirements to:

- ensure that an individual can find out about the personal information handling practices of council (e.g. through a Privacy Policy)
- take reasonable steps to make people aware of certain matters before collecting their personal information (e.g. through a Collection Notice).

Although not required under the IP Act, councils can benefit from proactively disclosing other information to the community about the way council handles or makes decisions relating to personal information (e.g. details of PIAs completed by council).



Practical guidance

Benefits of proactive disclosure

Proactive disclosure of council personal information handling practices can:

- deepen community understanding and awareness of how council makes decisions relating to personal information
- increase community understanding of the value in providing their information (e.g. where personal information is required in exchange for a council service)
- enhance community trust in council's personal information handling practices
- build community awareness of council projects that will collect and handle their personal information
- educate the community about how technology projects will work, including what personal information and data they will collect and how that data will be used
- assist councils in addressing negative community perceptions about council projects
- support ongoing community engagement and involvement with council (e.g. where community feedback is sought in relation to council initiatives)
- reduce volume of formal RTI and IP access applications by placing relevant information about council's personal information handling practices in the public domain.

To enhance transparency, messaging that is provided to the community through proactive disclosure should always be clear, well-structured and use language that is easy to understand.

Opportunities for councils to explore include publishing:

1. **strategy** – council documents that outline council's position on privacy, such as a privacy strategy, privacy management framework and plans
2. **extracts** – filtered categories of council's Personal Information Register (discussed further in Personal information holdings), for example, those that detail what types of personal information council collects and where it is located
3. **key risk documents** – full versions or summaries of PIAs undertaken by council.
4. **project-specific material** – dedicated webpages, videos and brochures focused on privacy management for complex council projects, for example, technology projects that use AI, IoT, surveillance or facial recognition technologies.

Personal information holdings

A personal information holding is a grouping or repository of personal information that is used by council for one or more purposes. Common examples of a personal information holding include customer relationship management systems, human resources and payroll systems, and complaints registers. Where council collects and holds personal information, it must do so in accordance with the IP Act.

Councils collect and manage significant amounts of personal information, which is held in numerous locations and in a variety of formats. Council may store personal information holdings on site, at council-owned data centres or physical storage facilities, within cloud storage platforms or with contracted service providers.

Managing all personal information holdings in a manner that accords with the IP Act can be a significant challenge for councils if they do not have an accurate accounting of where those holdings are, what personal information elements they contain and who (operationally) is responsible for them.



Tips

1. Plan a body of work to document council's personal information holdings, ensuring that adequate resources are allocated.
2. Use the [Personal Information Register Template \(XLSX\)](#) to catalogue council's personal information holdings.
3. Ensure personal information held across all council departments is documented (e.g. council pools, libraries, human resources), including where personal information has been collected by technologies and surveillance.
4. Ensure personal information held by service providers (including by cloud, electronic and physical storage providers) are documented in the Personal Information Register.
5. Implement processes to ensure that the Personal Information Register is regularly reviewed and updated to reflect changes in personal information holdings, or new holdings of personal information.



Local government obligations

Where councils collect personal information to fulfil one or more of their functions, they must comply with the requirements of the IP Act and the IPPs. This includes fulfilling:

- [Section 33](#) requirements in relation to the transfer of personal information overseas
- requirements of Chapter 2, Part 4 in relation to contracted service providers
- collection, use, disclosure, storage and security requirements of the IPPs
- requirements to provide access to and correction of an individual's own personal information.



Practical guidance

Personal Information Register

A Personal Information Register is a tool that councils can use to document their personal information holdings and key information about those holdings.

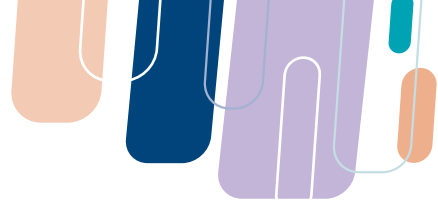
The OIC provides a [Personal Information Register Template \(XLSX\)](#) that councils can use to document their personal information holdings. The register contains fields that are relevant for all councils to complete, as well as optional fields relating to personal information management and risk. It also contains council-specific examples to assist in completing the relevant fields.

To complete the register:

- 1. Determine who** – nominate a coordination point for the completion of the register, which may involve:
 - o an officer or team responsible for completing the register
 - o decentralised operations-related responsibility for completing the register (e.g. where each department or business area completes relevant sections).
- 2. Decide what** – consider which aspects of the register council can comfortably complete now (with a view to adding in optional fields in future).
- 3. Set a timeframe** – allocate a period of time for initial completion of the register.
- 4. Plan next steps** – diarise ongoing review, updates and additions to the register.
- 5. See privacy opportunity** – be prepared to acknowledge and address privacy risks that come to light in relation to council personal information holdings.

Accurate completion of the Personal Information Register will allow councils to:

- record details regarding the system and storage location of each personal information holding
- record the types of personal information held at council data storage locations
- record details regarding the purpose for, and the method of, the collection of personal information
- record details regarding authorised access, and the sharing of personal information with other departments and external parties
- more effectively process access and correction requests
- publish data from the Personal Information Register, to better inform the community about the personal information held and the purposes for holding personal information, as part of proactive disclosure under the RTI Act
- facilitate a review of personal information holdings to ensure they remain accurate, complete and up-to-date based on the purpose of collection
- identify function-creep associated with the use of some personal information holdings



- where applicable, and in accordance with council policies, streamline the classification of data/information
- more easily identify privacy risks relating to the management of each personal information holding, including in relation to unnecessary collection, security of personal information, and contracted service providers involved in the management of personal information.



More information

- [Personal information register template \(XLSX\)](#)

Contracted service providers

A contracted service provider is defined in [section 34](#) of the IP Act. A contracted service provider is an entity that enters into a contract or other arrangement with council to provide services associated with one or more of a council's functions.

Councils are required to take all reasonable steps to bind service providers to comply with the privacy requirements set out in the IPPs and section 33 of the IP Act (i.e. obligations in relation to the transfer of personal information outside Australia).



Tips

1. Identify whether service providers will deal with personal information as part of providing services to or on behalf of council.
2. Enter into an agreement with service providers who will deal with personal information that requires compliance with relevant provisions of the IP Act.
3. Consider whether additional provisions should be included in the agreement (e.g. about subcontractors, privacy breach events, access and correction requests, performance reviews).
4. Implement mechanisms to monitor service providers to ensure they handle personal information in accordance with agreements. Do not just 'set and forget'.



Local government obligations

Chapter 2, Part 4 of the IP Act sets out obligations when engaging service providers, where the service provider will deal with personal information as part of providing services to or on behalf of council. Under section 34(2)(a), the services provided must be for the purpose of the performance of one or more of council's functions.

When engaging service providers, section 35(1) of the IP Act requires that councils take all reasonable steps to bind providers to the IPPs and section 33 of the IP Act (i.e. obligations regarding the transfer of personal information outside of Australia). Councils generally do this by entering into an agreement or contract with the service provider that places the same privacy obligations on the service provider as apply to council.

Requirements set out in Chapter 2, Part 4 do not apply if council is engaging a service provider where personal information is not involved in the provision of goods or services, such as the provision of grounds keeping, office cleaning or maintenance.



Practical guidance

Service providers often collect, use, store, process, analyse, disclose, exchange, share and otherwise handle personal information as part of providing their services to or on behalf of council. Service providers may, for example, provide services relating to data storage, cloud platforms or services, payment processing, and data or web analytics.

The IP Act requires that councils take all reasonable steps to ensure a service provider complies with relevant sections of the IP Act. In doing so, the best practice outcome is that a service provider collects and handles personal information 'as if it were council'. To this end, councils should enter into an agreement that binds service providers who deal with personal information to the IPPs and obligations regarding the transfer of personal information outside Australia.

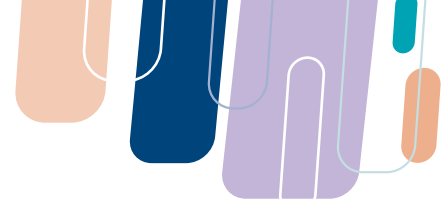
Councils may find benefit in reviewing the following resources that provide comprehensive examples and guidance for how privacy considerations can be addressed in a service arrangement. Councils may use these resources to guide the drafting or revision of their own agreements with service providers:

- [Queensland Government Service Agreement \(PDF\)](#)
- [Queensland Government Guidance: Create an ICT Contract.](#)

To ensure councils do not miss this opportunity:

- **assess privacy risk** – determine whether a project proposed to involve a service provider includes personal information handling by the service provider. A simple tool to help with this is [Privacy Threshold Assessment 'At a Glance' \(PDF\)](#)
- 1. **make privacy part of procurement processes** – build privacy checks into procurement processes, where potential service providers are made aware of council's requirements and given an opportunity to demonstrate that they are doing so at key junctures. Have a clear process for dealing with service providers who fail to adhere to agreed privacy requirements
- 2. **check in regularly** – do not 'set and forget' agreements with service providers. Councils should check that providers are handling personal information in the agreed manner. Where service providers are not acting in accordance with an agreement, activate the relevant procurement process
- 3. **avoid off-the-shelf services that do not contain adequate privacy safeguards** – such as those relating to document management, social engagement, opinion polls or surveys. Off-the-shelf agreements involve council agreeing to terms and conditions set by a provider, where there is no opportunity for council to negotiate privacy expectations associated with the service.

This does not include off-the-shelf services where personal information is not involved in the provision of products or services (e.g. the provision of certain software). Council may also be able to tailor its use of off-the-shelf services in such a way that excludes personal information (e.g. anonymous opinion polling).



Where off-the-shelf services are being considered, councils should conduct a [Privacy Impact Assessment](#) that – at a minimum – addresses:

- whether the provider’s privacy policy adequately explains how personal information is managed through its life cycle, including whether there is a dedicated ‘privacy’ contact for questions, complaints or to report a privacy breach
- whether the provider’s privacy policy, terms and conditions and other available documentation provide sufficient assurance to council that, in using the service, council will not contravene the IPPs or section 33 of the IP Act (i.e. in relation to the transfer of personal information outside Australia)
- the extent to which the provider’s terms and conditions:
 - o reflect responsible information practices
 - o offer council a reasonable opportunity to dispute the provider’s compliance with their own terms
 - o permit council to terminate the service without notice in the event of a privacy breach or other concern about personal information handling
 - o provide for the return or secure destruction of personal information upon termination or expiry of the service
- the provider’s reputation in the marketplace, and whether they are included in recognised supply arrangements for local government
- the cloud or physical storage locations used by the provider and any subcontractors, and whether the location is in a jurisdiction with a privacy law containing substantially similar requirements to those of the IP Act.

Councils should consider a dedicated sign-off process for off-the-shelf services, whereby officers with key accountability (such as the Executive Leadership Team or a dedicated committee) determine that the privacy risks posed by using a particular off-the-shelf service are acceptable to council. This supports accountability in decision-making and council’s ongoing assessment and management of privacy risks.



More information

- [Contracted service providers](#)

Assessing and managing privacy risks

Identifying, assessing, documenting and managing privacy risks is an important aspect of ensuring privacy compliance. Doing so also supports councils in reducing or removing impacts that may adversely impact the community.

Privacy risks may not always be obvious to council in the first instance – for example, those posed by council ‘data initiatives’ involving collation and publication of data, combining datasets internally within council, and sharing of datasets with external bodies for research purposes.



Tips

1. Complete a [Threshold Privacy Assessment](#) for all new projects or projects that change the way personal information is collected, used, disclosed, stored, secured or otherwise handled by council.
2. Undertake a [Privacy Impact Assessment](#) for all projects, where determined by the Threshold Privacy Assessment. A PIA identifies and assesses privacy risk and identifies recommendations to reduce or remove identified risks.
3. Implement PIA recommendations before deploying projects to ensure risks are reduced or removed before the collection or handling of personal information by the project.
4. Implement a Privacy Risk Register to document and manage identified privacy risks.
5. Actively manage privacy risks documented in the Privacy Risk Register, including those identified as part of the PIA process.
6. Establish policies and processes that set expectations and procedures to assess and manage privacy risks at council and integrate with council’s project development and management processes.
7. Raise staff awareness about privacy risk assessment and management processes, including with staff who are involved in project development.



Local government obligations

Councils have an obligation to ensure their handling of personal information is in accordance with the IP Act and the IPPs. Councils must also make decisions that are compatible with an individual’s human rights (e.g. the human right to privacy).⁵

Decisions in relation to accepting or managing privacy risk must be made with an individual’s right to privacy as a central consideration.



Practical guidance

Privacy Impact Assessment

Councils should assess the privacy risks of all new projects that involve personal information. This is generally known as a Privacy Impact Assessment (PIA). This is a due diligence exercise that examines privacy risk in the context of projects, including programs, processes, technologies, surveillance and other initiatives involving personal information.

PIAs help councils to make good decisions in respect of the handling of personal information by projects. When completed regularly, PIAs also serve to elevate the profile of privacy as part of council's culture and everyday practice. PIA processes should be integrated with project management and development processes of council.

In brief, the PIA process includes:

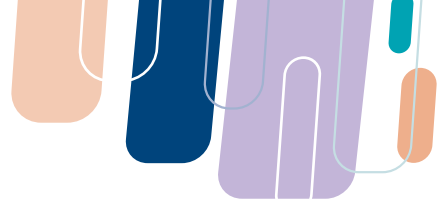
- 1. Threshold Privacy Assessment** – as a first step, a Threshold Privacy Assessment should be completed for each new project to determine whether a formal PIA is required.
- 2. Privacy Impact Assessment** – where determined by the Threshold Privacy Assessment, a PIA should be conducted, either internally by council or externally by a privacy expert. A PIA is a tool that councils can use to assess the privacy impacts of a new project and identify ways in which the obligations set out in the IP Act can be met.
- 3. Implement PIA recommendations** – before deploying projects, council should implement the recommendations of the PIA to reduce or remove identified privacy risks. Implementing recommendations before deployment assists councils to ensure privacy compliance in the context of their projects.
- 4. Respond and review** – councils must monitor the implementation of the PIA recommendations, and ensure the PIA is updated as changes are made to the design and implementation of the project.

Privacy risk management

Councils should implement processes to ensure the ongoing management of privacy risks. They may do this using a Privacy Risk Register. OIC offers a [Privacy Risk Register Template \(XLSX\)](#) that councils can use to record privacy risks, including those that have been identified as part of the PIA process and through completion of the Personal Information Register (which accounts for council's personal information holdings).

The register allows council to record a description of the risk, an assessment of the risk, the appropriate response to the risk and actions that will be taken by council to reduce or remove the risk. As first steps for completing the register, councils should:

- 1. Determine who** – nominate a coordination point for completion of the register, which may involve:
 - o an officer or team responsible for completing the register
 - o decentralised operations-related responsibility for completing the register (e.g. where each department or business area completes relevant sections).
- 2. Set a timeframe** – allocate a period of time for initial completion of the register.



3. **Plan next steps** – diarise ongoing review, updates and additions to the register.
4. **Set accountabilities** – where not already in place, nominate a responsible individual or role to be accountable for ongoing awareness and management of privacy risks at council.
5. **Decide a path** – where not already in place, determine how (and to whom) to escalate key privacy risks for decision-making.



More information

- [Overview of Privacy Impact Assessment \(PIA\)](#)
- [Threshold Privacy Assessment 'At a Glance' \(PDF\)](#)
- [Threshold Privacy Assessment Template \(DOC\)](#)
- [Guideline for undertaking a Privacy Impact Assessment](#)
- [Privacy Impact Assessment Report Template \(IPPs\) \(DOC\)](#)
- [Privacy Risk Register Template \(XLSX\)](#)

Surveillance technologies

Councils are increasingly using surveillance technologies to attend to several council functions, including city management and planning, safeguarding assets, land use surveys, local laws enforcement, environmental assessment and community engagement.

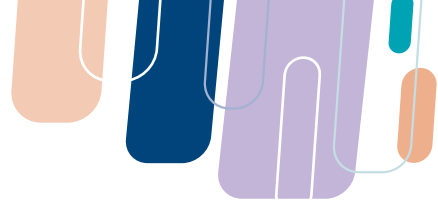
Councils are required to comply with the IP Act where surveillance technologies collect personal information. Some surveillance technologies that collect personal information include:

- closed circuit television (CCTV)
- facial recognition software
- body worn cameras
- drones
- internet or phone monitoring
- geo-location tracking
- sensors and cameras on council vehicles.



Tips

1. Complete a [Threshold Privacy Assessment](#) to determine if a [Privacy Impact Assessment](#) is required before deploying surveillance technology.
2. Clearly define the purpose of the surveillance technology and ensure that it aligns with council functions and activities.
3. Ensure the surveillance technology (and footage, recordings and data where it contains personal information) is only used for the defined purpose.
4. Implement other forms of Collection Notice to ensure people are aware of the collection of personal information (e.g. through the use of QR codes, signage, information published on council website).
5. Restrict staff access to surveillance equipment, footage, recordings and data that contain personal information.
6. Implement adequate security controls around surveillance equipment, and footage, recordings and data that contain personal information.
7. If using cloud-based storage to store surveillance footage, recordings or data, ensure the physical location of the storage, and any backups, are in Australia where possible.
8. Establish processes to deal with requests to access surveillance footage, taking into consideration requirements under the IP and RTI Acts.
9. Set time limitations for the retention of surveillance footage, recordings and data, before they are securely deleted or de-identified, in accordance with Retention and Disposal Schedule requirements.
10. Implement policies and procedures for managing surveillance activities that incorporate privacy obligations.



Local government obligations

Councils are required to comply with the IP Act where surveillance technologies collect personal information. Councils must also make decisions in a way that is compatible with human rights (including an individual's right to privacy) and give proper consideration to a human right when making a decision.

In using surveillance technologies, Councils must ensure that:

- the collection of personal information by surveillance technologies is necessary for the purpose of the project⁶
- where practicable, people are provided with a Collection Notice before their image or other personal information is collected using surveillance technologies (or as soon as practicable after the collection)⁷
- surveillance footage, voice recordings and other data are protected against loss, unauthorised access, use, modification or disclosure, or any other misuse⁸
- anyone can apply to access information included in footage, voice recordings and other data collected by surveillance technologies⁹
- surveillance footage, voice recordings and other data that contain personal information are only used and disclosed for the purpose that they were collected for.¹⁰ Where footage is to be used or disclosed for another purpose, council must determine whether an exception set out in the IPP 10 or 11 applies
- where surveillance footage, voice recordings and other data are provided to third parties, all reasonable steps are taken to ensure the third party will not use or disclose the information for a purpose other than the purpose that the information was provided to them.¹¹



Practical guidance

There are a number of opportunities for councils to ensure they are using surveillance technologies in a way that complies with the IP Act and takes account of community expectations.

⁶ Refer to IPP 1(1)(b)

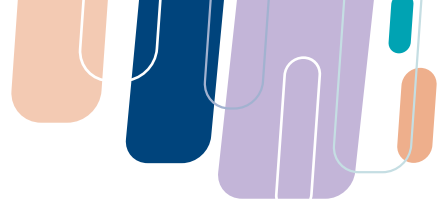
⁷ Refer to IPPs 2(3) and (4)

⁸ Refer to IPP 4

⁹ Refer to IPP 6 and Chapter 3 of the IP Act

¹⁰ Refer to IPPs 10 and 11

¹¹ Refer to IPP 11(3)



Complete a Threshold Privacy Assessment for all new projects, including new surveillance technologies. A Threshold Privacy Assessment will assist council to determine whether a PIA is required.

Conduct a Privacy Impact Assessment

To the greatest extent possible, councils should publish completed PIAs on their websites to enhance community awareness.

A PIA is a due diligence process that will assist council to:

- recognise privacy risks or impacts of surveillance projects
- identify actions that can be taken by council to reduce or remove the privacy risks and impacts associated with the project.

Due to the nature of surveillance technologies and the associated privacy challenges, a PIA will generally be required to be completed for any surveillance technology. Councils may choose to undertake a PIA internally or engage an external privacy expert to undertake a more comprehensive assessment. Undertaking a PIA, and implementing PIA recommendations, will ensure that privacy has been considered and acted upon before the deployment of surveillance devices.

The OIC has a number of PIA resources available. Refer to the Assessing and managing privacy risks section of this resource booklet.



Establish a clear purpose for using surveillance technology – that is, understand the problem council is trying to solve first, then determine whether surveillance technology is the best solution for addressing the problem.

Define the purpose

Prior to deploying any surveillance technologies, councils must determine what the surveillance intends to achieve, and ensure that this purpose relates to council functions. Councils should consider whether the surveillance technology is necessary to achieve the established purpose, or if the purpose can be achieved in another, and potentially less intrusive, way.

Once surveillance technology is deployed, councils must ensure that the surveillance technology, and captured footage and recordings (where they contain personal information), are not used for any other purpose, unless an IPP 10 exception allows the secondary use. This is vital for reducing instances of function creep; that is, widening the use of technology beyond its original purpose to the detriment of privacy.

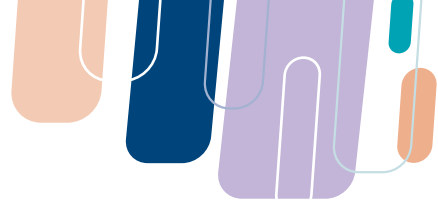


Notify the community through a Collection Notice.

Collection Notice

Providing a Collection Notice that informs people when their personal information is to be collected by surveillance technologies can be challenging. Councils should consider providing other forms of notice in these instances, including, for example, through the use of icons, QR codes, signage, public advertisements or by publishing information on the council website.

For more information about Collection Notices, see the Providing a Collection Notice section of this resource booklet.



Ensure adequate security controls are in place to ensure that personal information collected through surveillance technologies is protected against misuse, loss, and unauthorised access, use and disclosure. This includes placing controls around surveillance equipment, control rooms, real-time footage, and stored footage, recordings and data.

Implement security controls

In many cases, a PIA will help councils identify where there are security deficits to be addressed before surveillance technology is deployed.

Security controls councils should consider:

- placing physical security around surveillance equipment (e.g. housing for digital recorders, installing cameras out of reach)
- restricting access to surveillance control rooms and physical storage areas, using locks or swipe cards for access
- restricting staff access to stored surveillance footage, recordings and data, ensuring that access is only provided to limited staff who require it to undertake their roles
- keeping a record of access logs to surveillance equipment, control rooms and stored footage
- storing and transferring surveillance footage, recordings and data in an encrypted form
- where surveillance footage, recordings or data are to be stored in the 'cloud', ensuring the physical data centre or server (and any backups) are stored in Australia
- securely deleting or de-identifying surveillance footage, recordings and data when they are no longer required
- following established processes (where available) when responding to requests for access to surveillance footage.



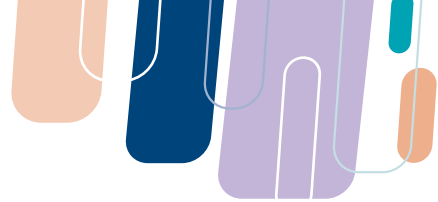
Informational videos, targeted media releases, static or interactive surveillance location maps and a dedicated webpage about council surveillance programs are all options for proactive disclosure of general information.

Develop processes for external access

In combination with these, establish processes for managing formal requests for access to surveillance footage, recordings and data, and publish this information on council's website.

Councils have obligations under the IP Act and the RTI Act to ensure that people can exercise their right of access to council information, including surveillance footage, unless on balance it is contrary to the public interest to give the access. Councils may receive requests from individuals (whose image has been captured), other people, organisations, insurance companies and law enforcement agencies.

Responding to access requests can be a complex process. Council will need to take account of factors including the manner of collection and storage used by the technology so that it can be accessible and searchable, the number of individuals who may be captured in the footage, and the number of ways in which a request can be handled (i.e. administratively, or under the RTI or IP Act).



Council information should, where possible (and with due consideration of the privacy rights of individuals whose personal information may be included in any footage, recordings and data), be given through informal means like council's website and other publications, publication scheme or through administrative release. A formal application for council-held information under the RTI or IP Act should be made as a last resort.



Establish timeframes for retaining surveillance footage, recordings and data (where they contain personal information), including a schedule for destroying or de-identifying the information.

Establish time limitations

When establishing time limitations for surveillance footage, councils should consider:

- when the footage will be no longer be necessary to fulfil the purpose of the surveillance project
- council obligations under the *Public Records Act 2002* and the relevant Retention and Disposal Schedule.

Securely destroying or de-identifying surveillance footage, recordings and data in a timely manner will help protect personal information from a privacy breach.



Consider establishing and implementing a specific governance framework to support privacy management in the context of council surveillance projects.

Implement policies and procedures for surveillance projects

A governance framework – inclusive of plans, policies, procedures and processes relating to surveillance technologies (whether as a whole, or in relation to each technology uniquely) – can assist councils with consistent decision-making in respect of privacy.

A governance framework should include processes to ensure the efficient and effective management of privacy breaches, in the event that surveillance footage, recordings or data that contain personal information are accessed, used, modified or disclosed without authorisation, or are lost or misused.



More information

- [Managing access to Digital Video Recordings](#)
- [Drones and the Privacy Principles](#)
- [Camera Surveillance and Privacy](#)



Council awareness of privacy issues

Councils may be alerted to privacy issues in a number of ways, including internally by council staff, notification by contracted service providers, or privacy queries or complaints from the community.

Council awareness of privacy issues is vital for ongoing improvement of privacy practices and maintaining trust of the community. Two common ways councils are alerted to privacy issues are:

- a privacy complaint
- notification by staff member or a contracted service provider.

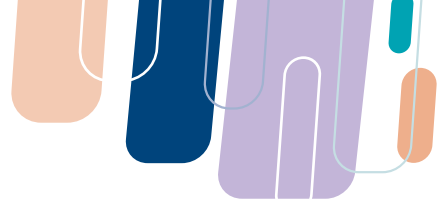
Privacy complaints

Individuals have the right to make a privacy complaint where they feel that a council has handled their personal information in a way that is inconsistent with the requirements of the IP Act. Councils have an opportunity to build community trust, and improve their personal information handling practices, where privacy complaints are handled in an appropriate manner.



Tips

1. Identify whether the complaint is about how council has handled personal information (i.e. is it a privacy complaint?).
2. Ensure privacy complaints are adequately investigated to determine whether council has complied with its privacy obligations.
3. Ensure ongoing communication with the complainant about the progress of their complaint and outcomes of council's investigations.
4. Treat all complainants with respect, and work with them to resolve the matter in an amiable and professional manner.
5. Where investigations uncover that council has handled personal information in a manner that is inconsistent with the IPPs or other requirements, implement measures to ensure compliance with privacy obligations in the future.
6. Where council has interfered with a person's privacy, offer the complainant an apology and explain the measures that council is taking to rectify the issue.



Local government obligations

Under Chapter 5 of the IP Act, individuals are able to make a privacy complaint where they feel that council has collected or handled their personal information in a manner that does not accord with requirements of the IP Act. If, after 45 days of making a privacy complaint, an individual is not happy with council's response or if council fails to respond to the complaint, the complainant is able to take their complaint to the OIC.



Practical guidance

What is a privacy complaint?

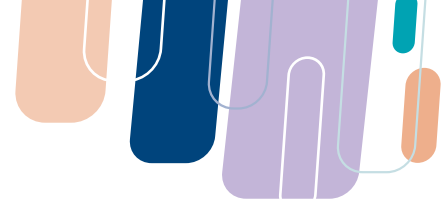
A privacy complaint is a complaint by an individual about an act or practice of a relevant entity (the respondent to the complaint) in relation to the individual's personal information that is a breach of the relevant entity's obligation under this Act to comply with (a) the privacy principles.¹²

When an individual complains about the collection or handling of their **personal information** by council, this is a privacy complaint.

Sometimes privacy complaints will at first appear as service complaints or a concern that council has not been 'fair'. To help recognise whether a complaint may be a privacy complaint, consider whether the complaint is about:

1. **Collection** – the collection of personal information by council
2. **Handling** – council's use or disclosure of the individual's personal information
3. **Accuracy** – council used information that the complainant states is inaccurate, out-of-date or incomplete
4. **Security** – security or storage of a personal information held by council
5. **Transfers** – the transfer of personal information outside of Australia
6. **Service providers** – the handling of personal information by council's contracted service providers
7. **Access** – a refusal of council to give access to, or correct, an individual's own personal information.

Identifying whether a privacy breach has occurred can sometimes be complex. Just because someone complains about council's handling of their personal information does not mean that council has handled personal information in a manner that does not comply with the IP Act. However, where an individual has raised a privacy complaint, and council has determined that it has not breached its privacy obligations, it is still important that council communicates with the complainant and addresses their concerns.



Appropriate handling of privacy complaints

It is important that local councils appropriately investigate and respond to privacy complaints that are made in relation to their personal information handling practices.

Appropriate handling of privacy complaints can assist councils to:

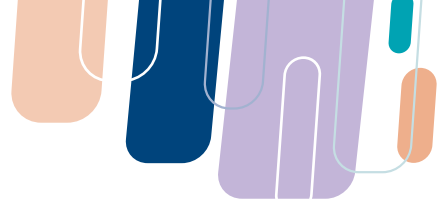
- identify whether council has interfered with the complainant's privacy by handling their personal information in a way that does not comply with the IPPs or other IP Act requirements
- identify potential privacy breach events, where personal information has been accessed, used, modified or disclosed without authorisation, or has been lost or misused
- reduce and remove future occurrences of the same type identified in the privacy complaint
- rebuild community trust and confidence in council operations
- avoid the involvement of the OIC and Queensland Civil and Administrative Tribunal and additional resources involved with same
- avoid referrals to the Office of the Independent Assessor or the Crime and Corruption Commission, these investigations, while important, can consume significant council resources.

Councils may implement processes to ensure that privacy complaints are investigated and responded to in an appropriate and consistent manner. OIC resources on privacy complaints management detail the following key processes:¹³

- 1. Identify** – determine if the complaint is a privacy complaint.
- 2. Acknowledge** – confirm receipt of the complaint.
- 3. Investigate** – investigate the issues raised by the complainant.
- 4. Respond** – contact the complainant to advise the findings of council's investigations and provide an invitation for the complainant to respond to the findings.
- 5. Remediate** – address the complaint, both internally and with the complainant directly.
- 6. Review** – learn from the issues raised in the privacy complaint and improve council privacy practices accordingly.

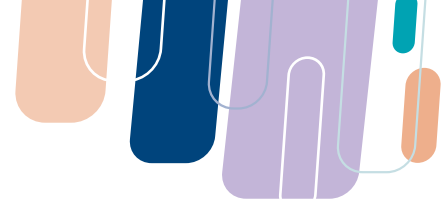
It is important that councils treat all complainants with respect. Not only do individuals have a right to have their concerns addressed, but the outcome of the complaint may also be significantly improved when councils work with the complainant to resolve the matter.

It is also important that councils meet statutory timeframes when dealing with access applications. There are legislated response times if you receive an application for access or amendment of personal information in a document in the council's possession. Not only will a timely response to the matter demonstrate that you are treating the applicant and their application with respect, but also not responding within the legislated time frame can result in a 'deemed decision' – an assumption that the council has refused access which can trigger the applicant then seeking an external review of this 'refusal' with the OIC.



More information

- [Privacy Complaint Management training video](#)
- [OIC and privacy complaints](#)



Privacy breaches

Privacy breaches occur when a council fails to comply with one or more of the IPPs, requirements in relation to transfers of personal information outside of Australia, or requirements in respect of service providers.

A privacy breach can result from technical issues, human error, inadequate resources and training, a misunderstanding of the law or deliberate acts.

A privacy breach may include (but is not limited to):

- over-collection of personal information (i.e. collecting more than is necessary for a council function)
- failure to take reasonable steps to notify an individual about the collection of their information
- refusal to give an individual access to their own personal information where no exception can be applied
- unauthorised use of personal information internally by council, or externally by third parties
- unauthorised disclosure of personal information, including where personal information is provided to service providers that have not been adequately bound to relevant sections of the IP Act
- transfer of personal information outside Australia in a manner that does not comply with the IP Act
- improper application of IPP exceptions in relation to the collection, use and disclosure of personal information; or where council acts as though it is relying on an IPP exception where no exception applies.

Councils may uncover privacy breaches in a number of ways, including as a result of investigations into privacy complaints.

One of the more common causes of a breach is the loss, theft, or unauthorised access, use, modification or disclosure of personal information. In accordance with best practice, and to promote openness and transparency, councils should notify the OIC and individuals affected by privacy breaches where they feel that the privacy breach is likely to result in a significant harm to the person whose privacy was breached.



More information

- [Responding to a potential privacy breach](#)
- [Privacy breach management and notification](#)
- [Privacy Breach Self-Assessment Tool](#)
- [Report a privacy breach to OIC](#)

Privacy program management

Establishing a privacy program, including policies, procedures and related processes, can support councils to consistently meet their privacy obligations.

A privacy program provides a structure that council staff can rely on when collecting and handling personal information, and may assist councils in implementing the practical guidance set out in this resource booklet.



Tips

1. Integrate privacy requirements into existing council policies and related programs to ensure personal information is valued and protected.
2. Establish policies, procedures and processes that relate directly to privacy, and reference privacy in complementary areas such as information security, records management, risk management, procurement and vendor management.
3. Regularly review council policies and processes to ensure ongoing alignment with IP Act requirements.
4. Socialise elements of the privacy program with council staff to ensure understanding and awareness of where privacy fits in to their work.



Local government obligations

Councils are required to comply with the IP Act and requirements of the IPPs in their collection and handling of personal information. A privacy program supports privacy compliance, improves privacy practices and influences a lasting privacy culture.



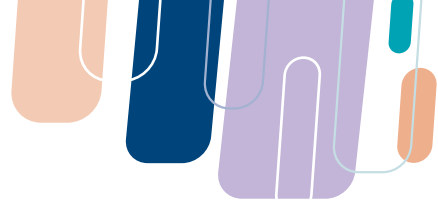
Practical guidance

A good privacy program considers the personal information handling requirements of council and how privacy relates to (and interacts with) different functions of council.

Privacy requirements should be integrated into policies, processes and procedures to ensure that personal information is valued and protected, in accordance with the IP Act and council's personal information handling practices as outlined in its Privacy Policy.

Policy areas related to privacy:

- access and correction of personal information
- privacy complaints management



- information security
- privacy breach management and notification
- business continuity and disaster management
- information or data classification
- records management and retention
- purchasing and procurement
- vendor engagement and management
- risk management.

Any privacy program implemented by council should be socialised within council to ensure staff awareness and understanding.



Staff privacy training and awareness

Privacy training and targeted messaging will assist councils in achieving best privacy practice. While a focus is on compliance, equally important is establishing a strong privacy culture within council.

Where councils do not have tailored privacy training in place, they can use OIC's [free general privacy awareness training](#) available online. This is a good starting point for councils to ensure staff have an understanding of key privacy concepts and obligations.



Tips

1. Conduct mandatory general privacy training for all staff at induction, and then at regular intervals thereafter.
2. Ensure privacy training accurately reflects IP Act and IPP requirements.
3. Tailor training to include key aspects of council's privacy program, including frameworks, policies and processes related to privacy and personal information handling.
4. Include an assessment component to all training to ensure staff understanding.
5. Document training attendance and completion.
6. Implement privacy messaging (e.g. posters, screen savers) to ensure ongoing privacy awareness.
7. Conduct targeted or specialist privacy training for relevant staff, including in relation to privacy complaint management, privacy risk assessment and acceptable use of ICT. Councils may contact the OIC if they have specific training needs in a targeted area.



Local government obligations

Local governments must ensure that personal information is collected and handled in accordance with the IP Act and requirements set out in the IPPs.

Privacy training and awareness messaging offer an opportunity for councils to communicate privacy obligations and expectations in relation to personal information handling.



Practical guidance

Council should consider implementing the following (using OIC privacy training and resources as required).

General all staff privacy training should be conducted as part of the induction process, and periodically thereafter. Councils may find benefit in blending privacy training with complementary areas, such as information security or code of conduct.

Messaging of key privacy requirements, including through the use of screen savers, posters and discussion points for meetings, will communicate that privacy is 'how we do things here'.

Targeted or specialist privacy training should be provided for certain roles, such as:

- roles involved in project management (e.g. privacy impact assessment training)
- roles that deal with the public (e.g. privacy complaints and access/correction request handling training)
- roles that handle ICT (e.g. training regarding the acceptable use of council ICT and information assets)
- management roles (e.g. how managers support council's privacy program).

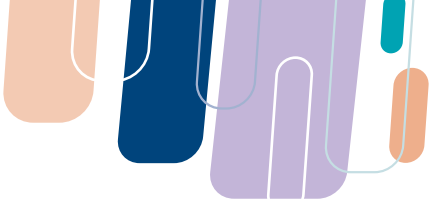
Implementing mandatory privacy training will assist council in raising privacy awareness and understanding within council of key privacy concepts, IP Act requirements and council's privacy program. Key privacy training requirements have been identified by the OIC and the Crime and Corruption Commission.¹⁴ These include:

- be mandatory and regular
- be monitored and followed up to ensure completion
- cover all relevant elements of information privacy and information security
- be accurate and consistent with the IP Act, any confidentiality and security obligations, and relevant policies and procedures
- be practical, contemporary and tailored to the local government context
- include an assessment component.

The OIC provides privacy [training and events](#) that councils may use, including online resources relating to:

- general *Information Privacy 2009 Act* awareness
- Privacy Complaint Management
- Privacy Impact Assessments
- access to information
- privacy and COVID-19
- misuse of information

¹⁴ The OIC Report No. 1 for 2018–19, Awareness of privacy obligations, and the Follow-up of Report No. 1 for 2018–19, Awareness of privacy obligations, Report No. 3 to the Queensland Legislative Assembly for 2020–21; and the Crime and Corruption Commission Operation Impala report.

- 
- decision writing
 - information sharing and the IP Act
 - managing and assessing re-identification risk.

The OIC also schedules a number of webinar and face-to-face training courses. Refer to the OIC's Training and events webpage to access these resources.

Council staff involved in privacy can [connect with OIC](#) to receive notifications on training and events by subscribing to OIC news and Practitioner network groups.



More information

- [Achieving effective privacy and information security training](#)
- [OIC Privacy Training and Events](#)



Privacy in multi-service environments

Councils may be part of a multi-service environment, especially those located in regional parts of Queensland. A multi-service environment includes two or more public agencies using co-located facilities and offices, such as where a council, law enforcement and health service agency share the same building.

Where a council is part of a multi-service environment, they must still adhere to privacy requirements of the IP Act, including those in relation to disclosure.



Tips

1. Document the personal information held (i.e. owned and controlled) by council. Council may use the [Personal Information Register Template \(XLSX\)](#).
2. Ensure all personal information held by council is stored separately from personal information held by other agencies.
3. Restrict access to personal information (including that held in physical and electronic format) to council staff who need it for their roles.
4. Implement processes to handle requests from the co-located agencies to access personal information held by council, including for the purposes of law enforcement.
5. Ensure that council does not access personal information held by other agencies other than in compliance with the IPPs.
6. Educate council staff (and where appropriate, staff of other agencies) about an agency's obligation to protect personal information from unauthorised access and disclosure.



Local government obligations

Under IPP 4 of the IP Act, local governments must protect documents that contain personal information from unauthorised access, use, modification or disclosure. Multi-service environments can create privacy challenges, particularly in relation to unauthorised disclosure.

The IP Act defines disclosure at s23(2):

An entity (the first entity) discloses personal information to another entity (the second entity) if –

- (a) the second entity does not know the personal information, and is not in a position to be able to find it out; and*
- (b) the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and*
- (c) the first entity ceases to have control over the second entity in relation to who will know the personal information in the future.*

Council would disclose personal information where it was shared with another agency, including those in a multi-service environment.

IPP 11 of the IP Act places limits on the disclosure of personal information. Councils must not disclose personal information unless an exception in IPP 11(1) applies. This requirement exists even where the information is being shared between public agencies in a multi-service environment.

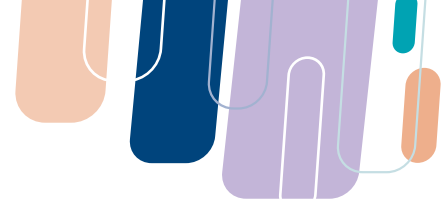


Practical guidance

Implement mechanisms to identify and understand what personal information council holds and then implement controls to ensure that personal information held by council is not accessed by or shared with other agencies within the same facility.

Council may use a Personal Information Register to identify and document personal information that it holds. The OIC provides a [Personal Information Register Template \(XLSX\)](#) to assist with this.

Council holds personal information where it has collected the information for the purpose of undertaking a council function or activity. Once council's personal information holdings have been identified, council must ensure that these are stored separately to holdings of other agencies. This includes where personal information is held in physical storage facilities, and electronic databases.



Access to separated council holdings must be restricted to **council staff** who require it to undertake their functions:

- 1. Restrict access** – restrict both physical access (e.g. keys, swipe cards) and electronic access (e.g. logins, 2 Factor Authentication) to personal information to authorised council staff.
- 2. Limit exposure ‘on the ground’** – personal information held in ‘temporary’ storage areas must be protected. This includes where personal information is held on loose paper documents on desktops, in drawers, physical inboxes and bins. Council must ensure that these documents cannot be accessed by staff from other agencies.

There may be times where council is authorised to disclose personal information to other agencies, as set out in IPP 11. To maximise accountability and promote community trust:

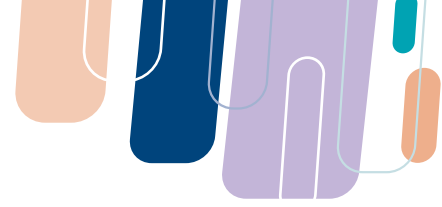
- 1. Set out a process** – even in a co-located environment, establish and implement processes to handle other agency requests to access personal information, including requests made by law enforcement agencies.
- 2. Put it in writing** – enter into an agreement with the relevant agency where it is proposed for information to be shared on an ongoing basis. The agreement must not place council in a position of contravening the IPPs.
- 3. Record disclosures** – make a notation of all disclosures to a co-located agency, including the reason and the relevant exception to IPP 11. This helps council to ensure that disclosures are made in a consistent and IPP compliant manner and establishes a record that a decision was made to provide personal information to the co-located agency.

Council staff (and where appropriate, other agencies within the multi-service environment) should be educated about their privacy obligations, particularly in relation to the disclosure of personal information and any processes and procedures that have been implemented.



More information

- [Personal Information Register Template \(XLSX\)](#)
- [Use and disclosure authorised by law](#)
- [Use or disclosure for law enforcement](#)
- [Use or disclosure for public interest research](#)
- [Use or disclosure to prevent harm](#)
- [Use or disclosure with agreement](#)
- [Disclosure where the individual was aware](#)
- [Privacy and information sharing between agencies](#)

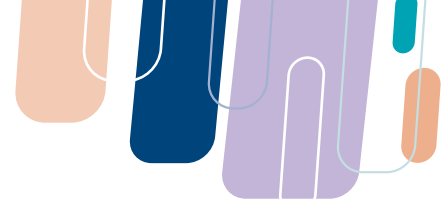


Appendix A: Glossary of terms abbreviations and acronyms

AI	Artificial intelligence, technologies that have the ability (or can be trained) to solve problems and make decisions.
CCTV	Closed circuit television, a television system in which video signals are transmitted from one or more cameras to a set of monitors.
Disclosure	An entity (the first entity) discloses personal information to another entity (the second entity) if (a) the second entity does not know the personal information, and is not in a position to be able to find it out; and (b) the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and (c) the first entity ceases to have control over the second entity in relation to who will know the personal information in the future, as defined in section 23(2) of the IP Act.
IoT	Internet of Things, including technologies and devices connected to the internet.
IPPs	Information Privacy Principles contained in Schedule 3 of the IP Act. The IPPs set obligations for the collection and handling of personal information.
IP Act	<i>Information Privacy Act 2009</i> (Qld).
Law enforcement agency	A law enforcement agency includes the Queensland Police Service; the Crime and Corruption Commission; the community safety department; or another agency, to the extent that it has responsibility for (a) the performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed, (b) the management of property seized or restrained under a law relating to the confiscation of the proceeds or crime; (c) the enforcement of a law, or of an order made under a law, relating to the confiscation of the proceeds of crime; or (d) the execution or implementation of an order or decision made by a court or tribunal, as defined by Schedule 5 of the IP Act.
OIC	Office of the Information Commissioner, Queensland.
Personal information	Information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, as defined by the IP Act.

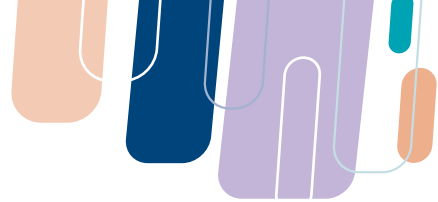


PIA	Privacy Impact Assessment. A PIA is a tool that councils can use to assess the privacy impacts of new project and identify ways in which the obligations set out in the IP Act can be met.
Privacy breach	A privacy breach occurs when council fails to comply with one or more of the privacy principles. One of the more common causes of a breach is the loss, theft, or unauthorised access, use or disclosure of personal information.
Privacy principles	As defined by Schedule 5 of the IP Act, ‘privacy principles’ means the requirements applying to councils under Chapter 2 of the Act; including the application of the IPPs, and requirements in regard to the transfer of personal information outside Australia (outlined in section 33) and contracted service providers (outlined in Chapter 2, Part 4).
Resource booklet	Privacy in local government.
Threshold Privacy Assessment	A Threshold Privacy Assessment is a preliminary assessment of a project to determine whether a formal PIA is required.
Use	An entity uses personal information if it (a) manipulates, searches or otherwise deals with the information; (b) takes the information into account in the making of a decision; or (c) transfers the information from a part of the entity having particular functions to a part of the entity having different functions, as defined in section 23(3) of the IP Act.



Appendix B: OIC privacy guidance, resources and training

Key privacy concepts	Overview of the Information Privacy Principles
	Personal information
	Key privacy concepts
Establishing a Privacy Policy	Access and openness obligations
Collection Notice	Collection Notice
Personal information holdings	Personal Information Register Template (XLSX)
Contracted service providers	Contracted service providers
	Queensland Government Service Agreement (PDF) (example)
	Create an ICT Contract (Queensland Government guidance)
Assessing and managing privacy risk	Overview of Privacy Impact Assessment (PIA)
	Threshold Privacy Assessment 'At a Glance' (PDF)
	Threshold Privacy Assessment Template (DOC)
	Guideline for undertaking a Privacy Impact Assessment
	Privacy Impact Assessment Report Template (IPPs) (DOC)
Surveillance technologies	Privacy Risk Register Template (XLSX)
	Managing access to Digital Video Recordings
	Camera Surveillance and Privacy
Council awareness of privacy issues	Drones and the Privacy Principles
	Privacy Complaint Management training video
	OIC and privacy complaints
	Responding to a potential privacy breach
	Privacy breach management and notification
Privacy Breach Self-Assessment Tool	
Report a privacy breach to OIC	



Staff awareness and training

[OIC Privacy Training and Events](#)

[Achieving effective privacy and information security training](#)

Privacy in multi-service environments

[Personal Information Register Template \(XLSX\)](#)

[Use and disclosure authorised by law](#)

[Use or disclosure for law enforcement](#)

[Use or disclosure for public interest research](#)

[Use or disclosure to prevent harm](#)

[Use or disclosure with agreement](#)

[Disclosure where the individual was aware](#)

[Privacy and information sharing between agencies](#)