Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Information sharing between agencies, information for law enforcement purposes, and information sharing in disaster events

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1.0 Overview

Queensland government agencies[1] must manage personal information in compliance with the privacy principles in the *Information Privacy Act 2009* (Qld) (**IP Act**). This includes when sharing personal information with other agencies or in response to critical events.

1.1 What are the privacy principles?

The Queensland Privacy Principles (**QPPs**) set the rules for how agencies collect, store, secure, verify, use, and disclose personal information and the rules for transferring personal information out of Australia.

Sharing personal information generally involves an agency disclosing personal information;[2] where the third party is another agency the QPPs governing collection[3] will apply to that receiving agency.[4] Sharing information with third parties that are not agencies is **not** addressed in this guideline. This guideline discusses information sharing between and with law enforcement agencies, and when agencies are managing disaster events.

[1] Agency includes a Minister.
[2] Disclosure is defined in section 23 of the IP Act. See Key privacy concepts - use and disclosure for more information.
[3] QPP 3
[4] QPP 3 does not apply to unsolicited personal information, i.e. the agency shares it with the other agency or agency with no prior discussion or permission. Unsolicited personal information must be dealt with under QPP.

Collection obligations

Agencies must not collect personal information unless it is reasonably necessary for one or more of their functions or activities and must collect it lawfully and fairly.[5] Generally, personal information must be collected from the individual concerned, and, if the information is 'sensitive information',[6] with the person's consent.

The QPPs can support the necessary flow of personal information between agencies, but the disclosing agency must consider its privacy obligations before deciding personal information can be shared.

Failure to comply with the QPPs can erode community trust and goodwill, cause distress and detriment to individuals, and result in privacy complaints. Privacy complaints which are not resolved by the agency can be escalated to the Office of the Information Commissioner and subsequently to the Queensland Civil and Administrative Tribunal, which can be costly and time consuming.

1.2 What is personal information?

The privacy principles apply to personal information. Personal information is any information about an identified individual or who is reasonably identifiable from the information.[3] All information that fits this definition is personal information, even if it does not seem sensitive or appears to be harmless, unimportant, or trivial. However, there are additional requirements if an agency wants to collect, use, or disclose sensitive information.[7]

If the information an agency wants to share is not personal information, the privacy principles do not apply. Refer to ***Key privacy concepts – personal and sensitive information*** for more information.

2.0 Sharing information between agencies

2.1 Benefits of sharing information

Agencies deliver services to the community in accordance with their specific responsibilities. Where these responsibilities overlap and/or interact with the responsibilities of other agencies, sharing information can aid in the efficient and effective targeting of government resources, support, and services.

Information sharing can lead to better informed government decision making and streamline government processes, particularly where the individual would otherwise be providing the same information to related agencies. This can be especially beneficial where the information may be difficult or traumatic to retell.

[5] QPP 3
[6] The concept of 'sensitive information' is defined in Schedule 5 of the IP Act.
[7] Refer to Key privacy concepts – personal and sensitive information for more information.

Sharing information can also provide enhanced protections for vulnerable members of the community, such as victims of family violence, by allowing better collaboration between support agencies.

2.2 Planning for information sharing

The steps an agency takes when planning to share information will depend on whether it will be one-off or an on-going arrangement.

Ongoing, regular sharing of personal information should be governed by a written agreement[8] that sets out the parameters of the arrangement, including the grounds on which the sharing is permitted, any limitations on access and use of that information, and a process to address situations where the agreement is not followed.

If information sharing will be a regular occurrence, this needs to be reflected in the information provided to individual under QPP 5.[9]

Addressing the below issues in an agreement can assist in ensuring the transferring agency and receiving agency meet their privacy obligations:

- Which officers will be involved in sharing the information before, during, and after? Generally, only officers who need to be involved in the process or subsequent use of the personal information should have access to the shared information.
- What is the nature of the information being shared? Is some or all of it sensitive or subject to specific security considerations?
- How is it being shared? This will often depend on the information's form, e.g., is it copies of paper or digital records or is partial/full access to an agency’s database being given?
- Is the sharing subject to audit or monitoring arrangements to ensure that the proposed objective is being/has been met and that only designated persons are involved in the process?
- Is there a timeframe for review of any long-term sharing arrangement?

Depending on the circumstances and information being shared, a privacy impact assessment (**PIA**) should be undertaken. A PIA will allow agencies to identify, assess, and manage any risks associated with the information sharing arrangement. Even if a PIA is not developed, assessing the risks associated with the intended information sharing can be an important part of privacy compliance.

One-off information sharing will generally not require a written agreement, but agencies need to consider their privacy obligations, decide whether sharing the information is appropriate, and document the disclosure.[10]

---

[8] For example, a Memorandum of Understanding.
[9] See guideline QPP 5 – Informing people when collecting personal information
[10] QPP 6 (6.5) requires that agencies disclosing under QPP 6 make a note of the disclosure with the information.

For both one-off and ongoing sharing, the disclosing agency and the receiving agency must ensure they comply with the relevant privacy principles.

Information sharing policies

A general information sharing policy that tells officers how to deal with requests for personal information from other agencies can help agencies meet their privacy obligations and safeguard against breaches.

A policy could set out the benefits of information sharing, explain the privacy considerations, include any disclosure request forms[11] or existing information sharing arrangements, and direct officers to more information and relevant contacts.

2.3 Sharing the information

As part of assessing any personal information sharing arrangement, agencies should identify:

- the purpose of sharing the information
- whether the sharing is authorised by an Act
- if disclosure is compliant with the QPPS, including whether it involves transferring it overseas.

A PIA can be useful for assessing and addressing these issues.

Human Rights Act

Agencies must also comply with the *Human Rights Act 2019* (Qld).[12] It requires agencies to give proper consideration to, and act compatibly with, human rights when making decisions or taking actions. This includes a decision to share, or not to share, personal information with another agency or agency.

2.3.1 What is the purpose of the information sharing?

It is essential that both the disclosing agency and the receiving agency understand and agree on the purpose of any proposed sharing of personal information. The purpose will determine:

- whether the agency requesting it can do so without breaching QPP 3; and
- whether the disclosing agency can share the personal information without breaching QPP 6.

2.3.2 Is there an Act that requires or permits the sharing?

[11] See, for example, QPS information request form
[12] See the Queensland Human Rights Commission for more info.

If an Act requires or permits the information to be shared, then the sharing will be authorised if it is done in accordance with any specific requirements in that Act.[13] This may require agencies to assess the Act to ensure its provisions have been complied with.

Example: information sharing arrangements

The *Domestic and Family Violence Protection Act 2012* (Qld) (**DFVP Act**) creates an information sharing arrangement that allows agencies[14] to share information where a person's safety may be at risk. It requires consent to be sought where safe, possible, and practical but allows sharing without consent where:

- the agency reasonably believes a person fears or is experiencing domestic violence; and
- the information may help another service receiving the information to assess whether there is a serious threat to the person's life, health, or safety because of domestic violence.

2.4 Required or authorised under a law or court order

Personal information can be used or disclosed where doing so is authorised or required by law, or by a court or tribunal order. This includes where it's impliedly authorised or required, because the agency cannot rely on the law or order without using or disclosing personal information.

2.4.2 If disclosure is prohibited by law

The QPPs **do not** override provisions of other Acts that prohibit the disclosure of personal information. If information is subject to confidentiality or secrecy provisions, agencies must refer to the relevant Act to determine if it can be shared.

2.4.3 Disclosure under QPP 6

Sharing personal information with another agency or agency will generally involve disclosing it.[15] Any disclosure of personal information to another agency or agency must either be the primary purpose of collection or be for one of the secondary purposes in QPP 6, which include:

- where the disclosure is related to the primary purpose of collection and the individual would reasonably expect it to be disclosed (for sensitive information, this must be a directly related purpose)

[13] Section 7(2)(b) provides that the IP Act gives way to other legislation that deals with disclosure; additionally, QPP 6.2(b) provides that personal information can be disclosed where it is authorised or required by law

[14] It also allows agencies and non-government entities to share information, but non-government entities are beyond the scope of this guideline. Refer to the DFVP information sharing guidelines for more information.

[15] Unless the other agency or agency already knows it or is in a position to find it out and/or the sharing agency will retain control of the information—see Key privacy concepts - disclosure for more information.

- with the individual's express or implied consent
- a permitted general or permitted health situation exists
- to prevent a serious threat to an individual or the public; and
- to a law enforcement agency or enforcement body to fulfill one or more enforcement functions.

Refer to the ***QPP 6 - use or disclosure*** for more information.

2.5 Disclosing information out of Australia

Any information sharing that requires personal information to be disclosed out of Australia will need to comply with section 33 of the IP Act. This includes where the individual has agreed to the disclosure, the disclosure is authorised or required by law, or is necessary to prevent a threat to an individual or the public.

For more information refer to ***Disclosing personal information out of Australia***.

2.6 Other privacy considerations: quality, relevance, security

Agencies are required under QPP 10.2 to take reasonable steps to ensure personal information agencies use or disclose is accurate, up to date complete and relevant.[16] Agencies intending to share personal information need to take these reasonable steps before disclosure .

Agencies should limit the information being shared to only what is necessary to fulfill the purpose of sharing and reasonable steps must be taken to protect the personal information from misuse, loss and unauthorised access, modification, or disclosure.[17] If it is no longer needed for any purpose, the agency must take reasonable steps to destroy or deidentify it, subject to relevant public records requirements.[18]

2.7 Privacy principle waivers

The IP Act allows for an agency's compliance with the privacy principles to be waived or modified where non-compliance is more in the public interest than compliance. These waivers can allow information sharing that would otherwise be a breach of the privacy principles, for example waiving the privacy principles to permit for information sharing between agencies to settle longstanding Aboriginal land ownership issues.[19]

Refer to ***Power of the Information Commissioner to waive or modify the privacy principles*** for more information.

[16] Refer to QPP 10 – Quality and accuracy of personal information for more information.
[17] Refer to QPP 11 – Security, deidentification and destruction of personal information for more information.
[18] ibid
[19] Waiver under section 157 of the Information Privacy Act 2009

3.0 Privacy and law enforcement agencies

3.1 The IP Act's law enforcement provisions

The IP Act contains a number of provisions dealing specifically with law enforcement agencies and enforcement-related activities. These provisions recognise that an agency's use of personal information for investigation and enforcement purposes may not be compatible with the privacy principles in all circumstances. For example, it would defeat the purpose of covert surveillance if an agency were required to inform the individual that their personal information was being collected.

Law enforcement agencies and enforcement-related activities are dealt with in three different ways in the IP Act:

- as part of the QPPs – agencies are bound by the QPPs but can rely on specific exceptions for law enforcement agencies and enforcement-related activities
- permitted non-compliance with some of the QPPs – an agency may be excused from complying with certain QPPs if necessary for an enforcement-related activity or other law enforcement function; and
- exemptions from the QPPs – the QPPs do not apply to personal information in specific documents.

3.2 Law enforcement agencies and enforcement-related activities

Law enforcement agency and enforcement-related activity are defined in schedule 5 of the IP Act.

This guideline is intended to be read in conjunction with ***QPP 3&6 - law enforcement agencies and activities***, which explains these in detail.

3.3 QPP 6 – use or disclosure

QPP 6.2(e) allow for the use and disclosure of personal information if the agency reasonably believes the use or disclosure is reasonably necessary for one or more enforcement-related activities conducted by a law enforcement agency.

If personal information is used or disclosed under QPP 6.2(e), QPP 6.5 requires the agency to make a written note of the use or disclosure.

QPP 6.2(f) allows an agency to disclose personal information to ASIO where all the requirements of QPP 6.2(f)(i)-(iii)are met.

Under QPP 6.2(b) personal information can be used or disclosed where the use or disclosure is required or authorised under an Australian law or a court or tribunal order. This is not limited to criminal proceedings, but it will apply in criminal or other enforcement proceedings before a court or tribunal.

Refer to ***QPP 6 – Use or disclosure*** and ***QPP 3&6 - law enforcement agencies and activities*** for more information.

3.4 Permitted non-compliance for law enforcement

Section 29 of the IP Act permits non-compliance by a law enforcement agency with specified QPPs. These are:

- QPP 3.6: the obligation to collect personal information only from the individual it is about
- QPP 5: the obligation to inform the individual of the matters listed in QPP 5.2 when collecting personal information
- QPP 6: the obligation to only use or disclose personal information for the purpose it was collected unless an exception applies; and
- QPP 10.1: the obligation to take reasonable steps to ensure personal information is accurate, up to date, complete and relevant.

Section 29(1) contains specific criteria that each specified law enforcement agency must satisfy before it can rely on section 29.

The law enforcement agency must also be satisfied on reasonable grounds that non-compliance with one or more of the specified QPPs is necessary in order to achieve or carry out the function in question. It is a decision that must be made every time the agency wishes to be non-compliant; it cannot, for example, decide as a matter of agency policy that all investigations into water pollution require non-compliance with one of the specified QPPs.

3.4.1 Enforcement related documents excluded from the privacy principles

Schedule 1 of the IP Act lists documents to which the privacy principles do not apply. Where those documents contain personal information, an agency does not have to handle it in compliance with the QPPs or the overseas disclosure rules in section 33. They include:

- Documents arising out of, or in connection with, a controlled operation or activity under the *Police Powers and Responsibilities Act 2000* (Qld) or the *Crime and Corruption Act 2001* (Qld).
- Documents arising out of, or in connection with, the covert undertaking of an operation, investigation or function of a law enforcement agency.
- Documents obtained under a warrant issued under the *Telecommunication (Interception and Access) Act 1979* (Cth).
- Documents to the extent they contain personal information about a person who is included in a witness protection program or is subject to other witness protection arrangements under the *Witness Protection Act 2000 (Qld).*
- Documents to the extent they contain personal information arising out of a complaint, or an investigation of corrupt conduct, under the *Crime and Corruption Act 2001* (Qld).
- Documents to the extent they contain personal information contained in a public interest disclosure under the *Public Interest Disclosure Act 2010* (Qld) or that has been collected in an investigation arising out of a public interest disclosure under that Act.

- Documents to the extent they contain personal information arising out of a complaint under the *Police Service Administration Act 1990* (Qld), part 7 or a complaint, or an investigation of corruption, under the *Crime and Corruption Act 2001* (Qld).

3.5 What if a law enforcement agency asks for personal information?

If a law enforcement agency (Agency One) requests information from any other Queensland government agency (Agency Two), Agency Two could rely on QPP 6.2(e) to disclose information to Agency One. However, Agency Two can only disclose if it is satisfied on reasonable grounds that the personal information is necessary for Agency One to carry out one or more 'enforcement-related activities' as defined in schedule 5 of the IP Act.

An agency which is asked to disclose personal information under QPP 6.2(e) must have sufficient evidence to satisfy itself that the disclosure is justified. In the event of a privacy complaint, the onus will be on the agency disclosing the personal information to demonstrate that it acted in compliance with the privacy principles. The agency may elect not to disclose personal information to a law enforcement agency under QPP 6.2(e) unless the request is made in writing by a sufficiently senior officer and sets out the reasons why the personal information is required.

Example
An enforcement officer from the Department of Safe Streets (the Department) attends the counter of the Queensland Bikes Board (QBB) and asks to see the records of Barry Bicyclist, because he "needs it to do his job". QBB does not have enough information to be sure that QPP 6.2(e) is satisfied.

QBB could request a senior officer of the Department to make the request in writing, giving enough detail to allow QBB to be sure disclosure would comply with the QPPs. If satisfied that disclosure was permitted, QBB could provide Barry's record to the Department. QBB would then have to make a written note of the disclosure.

If there is a regular, legitimate ongoing exchange of personal information between two agencies for law enforcement purposes – occurring consistently with QPP obligations then entering into a Memorandum of Understanding which sets out the requirements and procedures for each agency[20] will minimise the risk of a privacy breach.

4.0 Privacy and managing disaster events

This section of the guideline is intended to assist agencies which need to use, disclose, or access personal information in a disaster or emergency event. It includes practical tips and examples to increase understanding and help simplify compliance with the IP Act.

[20] Including an allocation of responsibilities, in the event of a data breach.

Disaster events include natural disasters, such as tropical cyclones, floods, bushfires and storms, and the serious disruption caused by the impact of a pandemic, all of which can directly affect the public's health, safety, and well-being.

Disaster events can exact a corresponding cost on communities and businesses, and impact government's ability to deliver services. The risk and impact of disaster events is exacerbated during Queensland's storm season[21] and flu season which carries an increased risk of an outbreak of human influenza.

4.1 What is a disaster?

A disaster is defined as:

> *…a serious disruption in a community, caused by the impact of an event, that requires a significant coordinated response by the State and other entities to help the community recover from the disruption.* [22]

A critical component of this coordinated response is the timely exchange of accurate, complete, and up to date information, including the personal information of all individuals affected by a disaster event and those involved in its management.

4.2 Can agencies share personal information in a disaster or an emergency situation?

There are privacy considerations whenever a Queensland government agency deals with personal information. While it is a common misconception that the privacy principles in the IP Act work against the sharing of personal information between agencies, the reality is that they not only provide generous flexibility for information exchange in disaster event circumstances, the privacy principles do so without compromising the privacy of that information once the disaster event has been dealt with.

Tip

The capacity to identify a person is a key component of personal information. Aggregated or de-identified data does not contain personal information and should be used where the identity of individuals is not necessary to achieve the intended purpose.

For example, sharing information that "*currently there are two people with diabetes, four pregnant people, two elderly people and five children on board and enroute to the evacuation centre*" would be sufficient for the evacuation centre to undertake support planning.

Information about an individual is distinct from information about things associated with an individual or even information of great interest to individuals. For example, a land map showing the extent of flooding in a particular area would

[21] between November and April – see http://www.bom.gov.au/cyclone/about/eastern.shtml.
[22] Section 13(1) of the *Disaster Management Act 2003*.

generally not be personal information, even though there would be individuals whose properties fall within the area shown on the map.

4.3 What flexibilities does the IP Act provide?

4.3.1 Collection notices

When an agency collects personal information, it must take reasonable steps to make the individual aware of the matters listed in Queensland Privacy Principle 5 (QPP 5) which are reasonable in the circumstances.[23] In the context of a disaster event, there may be no or few reasonable steps the agency can take, and many of the QPP 5 matters may not be relevant.

See ***QPP 5 – Informing people when collecting personal information***

4.3.2 Threats to life, health or safety and missing persons

An agency can use or disclose personal information to lessen or prevent a serious threat to the life, health, or safety of any individual, or to public health or safety where it's impracticable to obtain the individual's consent. This will be extremely relevant in disaster events, the nature of which will often making obtaining consent impracticable.

While it could appear limiting that the threat must be serious, Queensland's experience has shown that disaster events often have tragic consequences, meaning they will generally represent a serious threat. It is not necessary for the threat to be immediate or imminent, which allows this exemption to cover prevention; it can encompass steps taken to ensure that the threat does not eventuate.

If certain conditions are met, agencies can also use or disclose personal information if they reasonably believe doing so is reasonably necessary to locate a person reported as missing.[24]

4.3.3 Consent

Individuals can expressly or impliedly consent to a secondary use or disclosure of their personal information, including sharing their personal information with other agencies. An individual can also consent to their personal information being disclosed overseas, e.g., where an agency includes it in a social media post or update.

While it may be most common to seek consent when the agency wants to use or disclose the personal information, agencies could consider obtaining consent in advance of a disaster event, with the consent being relied on should a disaster occur.

[23] Refer to QPP 5 – Informing people when collecting personal information.
[24] The use or disclosure must ***also*** comply with the Commissioner's guidelines, which had not commenced at the time of writing. Refer to QPP 6 – use or disclosure.

4.4 What privacy protections are offered by the IP Act in the event of a disaster?

While the IP Act includes generous flexibilities which an agency can rely on in the event of a disaster, agencies must still deal fairly with personal information. Personal information can only be collected if it's reasonably necessary for, or directly related to, an agency's functions or activities. If an agency receives personal information it didn't request, the information must be assessed under QPP 4, to determine if retaining that personal information is appropriate.

Personal information must be secured and protected and can only be used or disclosed for secondary purposes in compliance with the IP Act, and individuals have the right to access or amend their personal information.

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published November 2024 and Last Updated 1 November 2024