Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Interpreting the legislation – Information Privacy Act 2009

QPP 3&6 – Permitted General Situations

Lessen or prevent serious threat to life, health or safety
Unlawful conduct or misconduct of serious nature
Locate a missing person
Defence of a legal claim
Alternative dispute resolution

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. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1.0 Overview

All Queensland government agencies[1] must handle personal information in accordance with the Queensland Privacy Principles (**QPP**) in the *Information Privacy Act 2009* (Qld) (**IP Act**).

This guideline is based on and includes material from the Australian Privacy Principle guidelines developed by the Office of the Australian Information Commissioner.

1.1 What is personal information?

Section 12 of the IP Act provides that 'personal information' means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion, whether it is true or recorded in a material form.

The individual does not need to be directly identified for the information to be 'personal information'. It is sufficient if they can reasonably be identified by reference to other information.

[1] References to an agency in this guideline include a Minister, bound contracted service provider, or other entity required to comply with the QPPs.

1.2 What is sensitive information?

'Sensitive information' is a category of personal information defined in schedule 5 of the IP Act, and includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation and criminal record. It also includes health, genetic and some biometric information.

Refer to ***Key privacy concepts – sensitive and personal information*** for more information.

2.0 Collection of sensitive information

An agency cannot collect sensitive information without consent unless one of the exceptions in QPP 3.4 applies. These exceptions include where a permitted general situation applies.

Refer to ***QPP 3 – collection of personal information*** for more information.

3.0 Use or disclosure

An agency can use or disclose personal information for the reason it was collected (the **primary purpose**). An agency cannot use or disclose personal information for a secondary purpose without consent, unless one of the exceptions in QPP 6.2 applies. These exceptions include where a permitted general situation applies.

'Use' and 'disclosure' are both defined in the IP Act.[2] Refer to ***Key privacy concepts – use and disclosure*** for more information.

4.0 Permitted general situations

As noted, both the QPP 3 restrictions on collecting sensitive information, and the QPP 6 limitations on secondary use or disclosure, are subject to exceptions, including where a permitted general situation applies.

The permitted general situations are listed in schedule 4, part 1 of the IP Act:

- lessening or preventing a serious threat to the life, health or safety
- taking appropriate action in relation to suspected unlawful activity or misconduct of a serious nature
- locating a missing person
- establishing, exercising or defending a legal or equitable claim
- confidential alternative dispute resolution process.

[2] Section 23 of the IP Act.

5.0 Lessening or preventing a serious threat to life, health or safety

5.1 Collection, use or disclosure to prevent a serious threat

An agency may collect sensitive information, or use and 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 is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure
- the agency reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety.[3]

5.2 Unreasonable or impracticable to obtain consent

Under the IP Act, consent can be express or implied. Refer to ***Key privacy concepts – consent*** (guideline under development) for information about what constitutes valid consent under the QPPs.

Before collecting sensitive information or using or disclosing personal information to prevent a serious threat, agencies must identify a clear reason why it is unreasonable or impracticable to obtain the individual's consent. Relevant considerations may include:

- The nature and potential consequences of the serious threat. For example, the urgency of a situation and level of harm threatened may require information to be urgently collected, used or disclosed in circumstances where there is no time to seek consent.
- Any possible adverse consequences to an individual if the agency collects, uses, or discloses their information without consent. The greater the adverse consequences, the more difficult it will generally be to establish it was unreasonable or impracticable to obtain their consent.
- The source of the threat. For example, it would generally be unreasonable to seek consent from the individual posing the threat, particularly where they would be unlikely to give it, or where seeking their consent could increase the threat or make it more difficult to prevent.
- Whether the individual can be contacted. For example, it will generally be impracticable to obtain consent if an individual's location is unknown or cannot reasonably be discovered, or if there is another reason they cannot be contacted, e.g., they are in a remote or disaster affected area with limited ability to receive communications. The number of individuals whose information is to be collected, used, or disclosed. It may be impracticable to obtain consent, for example, from a very large number of individuals (though see below as to the relevance of inconvenience, time, and costs).

[3] Schedule 4, part 1, permitted general situation 1(a).

- The inconvenience, time and cost involved in obtaining consent. However, it is not unreasonable or impracticable to obtain consent just because it would be inconvenient, time-consuming or involve a cost. Whether those factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

Capacity

Agencies need to consider whether an individual has capacity to give consent. Without capacity, an individual cannot consent, therefore it will generally be unreasonable or impracticable to obtain their consent.

However, if an individual has nominated a guardian or representative to provide consent on their behalf, the agency should consider whether it is impracticable or unreasonable to seek consent.

5.3 Reasonably believe collection, use or disclosure is necessary

Where it is unreasonable or impracticable to obtain consent, an agency must reasonably believe the collection, use or disclosure is necessary to lessen or prevent a serious threat. This is an objective test: would a reasonable person, who is properly informed view the collection, use, or disclosure of the personal information as necessary?

There must be a reasonable basis for the belief, and not merely a genuine or subjective belief. The onus lies with the agency to justify the basis for its belief.

5.4 Necessary

Part of deciding if the collection, use or disclosure is necessary involves making an assessment about whether the harm can be lessened or prevented without the information, e.g., by de-identifying personal information before disclosure or collection of de-identified information. If so, the collection, use or disclosure of personal information is not necessary.

It is not sufficient that an agency believes that a threat exists. It must reasonably believe that the collection, use or disclosure of personal information is necessary to lessen or prevent that threat. The following questions may assist agencies in making a determination:

- Is the information being collected, used, or disclosed with the intention of lessening or preventing the threat?
- Is the information being collected, used, or disclosed to manage the threat?
- When disclosed, is the recipient in a position to act on the information to lessen or prevent the harm?
- Will the proposed collection, use or disclosure of the information reduce the threat?

Agencies considering collecting, using, or disclosing information to reduce a threat to public health or public safety may find it useful to discuss the threat in

general terms (and whether the proposed collection, use or disclosure is likely to reduce the threat) with a relevant authority dealing with public health or safety, for example, a health agency or the agency responsible for environmental health.

5.5 A serious threat

The threat an agency is trying to lessen or prevent by collecting, using, or disclosing the personal information must be serious, and must involve a threat to an individual's life, health, or safety or public health or safety. The permitted general situation would not ordinarily extend to a threat to an individual's finances or reputation.

The likelihood of the threat occurring, as well as the consequences if the threat were to materialise, are both relevant when deciding if a threat is serious. A threat that could have dire consequences, but is highly unlikely to occur would not generally constitute a serious threat. However, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat. This allows agencies to take preventative action to stop a serious threat from escalating before it materialises.

The individual whose personal information is being considered does not have to be the one at risk of harm and the threat does not need to be to an identifiable person. It may be a threat of harm to be randomly inflicted, or inflicted on a class of persons, so that it is impossible to identify a specific person against whom the threat is directed.

'Health' includes mental health—mere stress, aggravation, or inconvenience is unlikely to constitute a 'serious threat' to health, however the triggering of a serious stress-related disorder may. For public health or safety—this must be a real and serious threat to the general public, or a portion of it, such as a bushfire or flooding threatening a locality.

The threat does not have to occur in Queensland or in Australia. It may happen anywhere in the world.

5.6 Can collection/use/disclosure prevent or lessen the serious threat?

Agencies must reasonably believe that the collection, use or disclosure of personal information will lessen or prevent the serious threat. This will generally require a sufficient link between the collection, use or disclosure of the information and the prevention or lessening of the threat.

In the case of disclosure, it would normally be to another government agency or body with the capacity and authority to reduce or prevent the threat.

5.7 Lessen or prevent

For a serious threat to be lessened or prevented, the collection, use or disclosure of personal information must allow the agency collecting, using, or receiving the information to take steps it would not otherwise have been able to take to either avoid or reduce the threat. It must be more than a mere chance of reducing the threat, or a 'just in case' measure.

If the attempt to lessen or prevent the serious threat is unsuccessful, it will not necessarily invalidate the collection, use or disclosure of the information, as long as the agency reasonably believes that collecting, using or disclosing the information would do so.

6.0 Unlawful activity or misconduct of a serious nature

6.1 Collection, use or disclosure where reason to suspect unlawful activity or misconduct

An agency may collect sensitive information without consent, or use and disclose personal information where the agency:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and
- reasonably believes that the use or disclosure is necessary for the agency to take appropriate action in relation to the matter.[4]

This permitted general situation will generally apply to an agency's internal investigations about activities within or related to the agency.

6.2 Reason to suspect

An agency must have 'reason to suspect' or a reasonable suspicion that unlawful activity or serious misconduct is being, or may be engaged in. The agency will bear responsibility for establishing a reasonable suspicion.

6.3 Reasonably believe collection, use or disclosure is necessary

An agency must reasonably believe the collection, use or disclosure of personal information is necessary for the agency to take appropriate action. As discussed above at 5.3, there must be a reasonable basis for the belief that the collection, use or disclosure is necessary, and not merely a genuine or subjective belief.

Assessing this issue requires the agency to consider whether the collection, use or disclosure will actually assist in achieving the purpose. Generally, the agency must:

- be satisfied that there is a link between the proposed collection, use or disclosure and the purpose; and
- establish that the link is sufficient to make the collection, use or disclosure of information necessary.

The collection, use or disclosure of the personal information need not be essential or critical to the activity, but it must be more than just helpful, desirable or expedient.

It is important to take a practical approach when making this determination. If an agency cannot effectively perform a function or undertake an action – such as

[4] Schedule 4, part 1 of the IP Act, permitted general situation 1(b).

taking appropriate action in relation to suspected unlawful activity or misconduct – without collecting, using, or disclosing information, there will generally be a reasonable basis to believe the collection, use or disclosure is necessary.

However, if alternative courses of action are reasonably available, for example, if deidentified information would be sufficient for the function or activity, it will be more difficult to establish a reasonable belief that the collection, use or disclosure is necessary.

Agencies cannot solely rely on normal business practice in assessing whether collection, use or disclosure of personal information is necessary. The primary consideration is whether, in the specific circumstances, there is a reasonable basis to believe that collection, use or disclosure is necessary.

6.4 Appropriate action

The action an agency reasonably believes is necessary must be an appropriate action to take in relation to the matter. This will depend on:

- the nature of the suspected unlawful activity or misconduct; and
- the nature of the action the agency proposes to take.

Appropriate action could include investigating the unlawful activity or serious misconduct, taking disciplinary action in relation to the unlawful activity, reporting the activity to the police, the Crime and Corruption Commission, or another relevant person or authority.

If the agency reasonably believes it cannot effectively investigate the serious misconduct or unlawful activity without collecting, using, or disclosing information, this permitted general situation will generally apply.

6.5 Related to the agency's functions or activities

The unlawful activity or serious misconduct must relate to an agency's functions. Generally, this will involve serious misconduct or unlawful activity undertaken by an agency's employees.

If the unlawful activity or serious misconduct relates entirely to an employee's private activities, e.g., the agency discovers the employee participated in illegal fishing while on holiday or engaged in serious misconduct in their role as board member of a private club, it cannot rely on this permitted general situation.

However, if the agency becomes aware that a non-employee, e.g., a contracted service provider, has engaged in serious misconduct or unlawful activity which relates to the agency's functions or activities, the agency may rely on this permitted general situation.

The function of an agency may be broadly defined under an Act and refined by Regulation, departmental or Council policy, Ministerial direction, government strategies or arrangements, or whole of government or whole of sector policies. Identifying an agency's functions requires a consideration of the instruments that

confer, describe, or apply to the agency's responsibilities and obligations. These can include:

- Acts and subordinate legislative instruments
- the Administrative Arrangements Orders
- government decisions or Ministerial statements that announce a new government function
- the agency's Publication Scheme; and
- the agency's Annual Report.

The activities of an agency will be related to its functions and include incidental and support activities, such as human resources, corporate administration, property management and public relations activities.

When considering whether something falls within a function or activity of an agency, a starting point is to ask: 'Can the agency legitimately do this under relevant legislation or organisational policy'? This includes not just the agency's outward facing mandates i.e., the functions it carries out for the community, but its inward facing ones, i.e., the functions it carries out with regard to its employees.

6.6 Unlawful activity

'Unlawful activity' generally means criminal activity, illegal activity, or activity prohibited or proscribed by law. It can include unlawful discrimination or harassment but does not include breach of a contract.

There is a crossover between unlawful activity and serious misconduct, which means in some instances an action may be both.

6.7 Serious misconduct

'Serious misconduct' refers to serious breaches of standards of conduct associated with a person's duties, and includes:

- corruption, abuse of power, or dereliction of duty
- breach of obligations that would warrant the taking of enforcement action against the person
- breach of trust
- breach of discipline; or
- other seriously reprehensible behaviour.

It does not include minor breaches or transgressions.

Whether the actions of an agency employee constitute serious misconduct will generally involve a failure to comply with relevant laws and standards, for example:

- corrupt conduct under the *Crime and Corruption Act 2001* (Qld)
- misconduct under the *Police Service Administration Act 1990* (Qld) or the *Public Sector Act 2022* (Qld)
- other conduct under section 91 of the *Public Sector Act 2022* (Qld) where it is serious and improper

- misconduct or corrupt conduct under the *Local Government Act 2009* (Qld) or breach of a Code of Conduct issued under that Act.
- a breach of the *Public Sector Ethics Act 1994* (Qld) or of a Code of Conduct under that Act; or
- a criminal offence.

Misconduct of this type may also be set out in an agency or sector specific laws.

7.0 Locate a Missing Person

7.1 Collecting, using or disclosing personal information to locate a missing person

An agency may collect sensitive information without consent, and use or disclose personal information if:

- an agency reasonably believes that collection, use or disclosure is reasonably necessary to locate a person reported as missing; and
- the collection, use or disclosure complies with a guideline issued by the Information Commissioner.[5]

The process for preparing, approving, and issuing a guideline for the purposes of a situation involving a missing person is set out in sections 44 and 45 of the IP Act. At the time of writing, these sections of the IP Act had not commenced and further information will be provided in relation to this permitted general situation following publication of any guideline by the Information Commissioner. These provisions are expected to commence on 1 July 2025.

8.0 Defence of a legal or equitable claim

8.1 A legal or equitable claim

Agencies may collect sensitive information and use or disclose personal information where the collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.[6] The phrase 'reasonably believes' is discussed above at 5.3 and 6.3. 'Reasonably necessary' requires that an agency consider whether a reasonable person, properly informed, would view the collection, use or disclosure as necessary.

This permitted general situation applies to claims conducted in both a court or tribunal, and to existing and anticipated legal proceedings. For anticipated proceedings, there must be a real possibility that they will commence, e.g., where an agency has sought or obtained legal advice about commencing a proceeding.

Agencies are not required, and may not be permitted, to disclose personal information to a third party who requests it in connection with an existing or

[5] Schedule 4, part 1, permitted general situation 1(c).
[6] Schedule 4, part 1 of the IP Act, permitted general situation 1(d).

anticipated legal proceeding. It will generally be difficult to establish that disclosure is reasonably necessary in these circumstances.

8.2 Subpoenas or other court orders

If a third party request is made in the form of a subpoena or other court order, QPP 6.2(b) will apply.

Refer to ***QPP 3&6 – authorised by law or court order*** (guideline under development) for more information.

9.0 Confidential alternative dispute resolution process

9.1 Collection, use and disclosure for alternative dispute resolution process

An agency may collect sensitive information without consent, or use or disclose personal information, where the collection, use or disclosure is reasonably necessary for conducting a confidential alternative dispute resolution (**ADR**) process.[7] As discussed above at 8.1, the phrase 'reasonably necessary' requires that a reasonable person, properly informed, would view the collection, use or disclosure as necessary.

9.2 A confidential ADR process

ADR, which is not defined in the IP Act, includes processes other than formal court or tribunal determinations in which an impartial person assists people in a dispute to resolve an issue. The impartial person may have ADR related accreditation, but this is not required.

Examples of ADR processes include mediation, conciliation, facilitation, expert assessment, determination or neutral evaluation.

Collection, use or disclosure for a confidential ADR process could include:

- collection of sensitive information necessary for the conduct of an ADR disclosure of personal information to an ADR provider
- use or disclosure by an agency for the purpose of participating in ADR; and
- collection of sensitive information, or use or disclosure of personal information, by an agency in relation to a complaint of professional misconduct against an ADR practitioner.

9.3 The ADR must be confidential

The parties to a dispute and the ADR provider must be bound by confidentiality obligations. The obligations must prohibit the use or disclosure of personal information collected, used or disclosed for the ADR process for any other purpose, including in subsequent proceedings.

[7] Schedule 4, part 1 of the IP Act, permitted general situation 1(d).

The confidentiality obligations may be imposed through binding agreements or legislative provisions. As an example of a legislative ADR confidentiality provision, see section 173A of the IP Act,[8] which provides for the confidentiality of privacy complaint mediations conducted by OIC.

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 August 2024 and Last Updated 01 August 2024

[8] To commence on 1 July 2025.