

---

## IPOLA GUIDELINE

### Interpreting the legislation – Information Privacy Act 2009

#### QPP 1 – Open and transparent management of personal information

**This guide does not reflect the current law.**

**It highlights important changes to the *Information Privacy Act 2009* in a general way.**

**This guide is not legal advice and additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.**

#### Overview

All Queensland government agencies<sup>1</sup> must handle personal information in accordance with the Queensland Privacy Principles (QPPs) 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.

#### ***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, whether it is true or recorded in a material format.

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

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

#### QPP 1

---

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

The object of under QPP 1, is to ensure agencies manage personal information in an open and transparent way<sup>2</sup>, where agencies must:

- take reasonable steps to implement practices, procedures and systems that will ensure it complies with the QPPs<sup>3</sup>, and is able to deal with related inquiries and complaints
- have a clearly expressed and up-to-date QPP privacy policy; and
- take reasonable steps to make its QPP privacy policy available free of charge and in an appropriate form (e.g., on a website).

### ***Implementing practices, procedures and systems to ensure QPP compliance***

QPP 1 requires an agency to take reasonable steps to implement practices, procedures and systems relating to the agency's functions and activities that will:

- ensure the agency complies with the QPPs; and
- enable the agency to deal with inquiries or complaints from individuals about the agency's compliance with the QPPs.

In addition to being a general statement of an agency's obligation to comply with the QPPs, QPP 1 requires agencies to take ongoing, proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the QPPs.

#### **Documenting implementation**

Agencies could consider keeping a record and publishing of the steps taken to comply with QPP 1 as a way of demonstrating that they are managing personal information in an open and transparent way.

### ***Reasonable steps***

The requirement that agencies implement practices, procedures and systems is qualified by a 'reasonable steps' test. What are reasonable steps will depend upon the circumstances, including:

- The nature of the personal information. More rigorous steps may be required as the amount and sensitivity of personal information increases.
- The possible adverse consequences for an individual if their personal information is not handled as required by the QPPs.

<sup>2</sup> Schedule 3 Part 1 (1.1) IP Act

<sup>3</sup> or QPP Codes issued under Chapter 3, Part 1 of the IP Act



More rigorous steps may be required as the impact of not handling the personal information increases.

- The practicability, including time and cost involved, of implementing them. A 'reasonable steps' test recognises that privacy protection must be viewed in the context of the practical options available to an agency. However, an agency is not excused from implementing specific practices, procedures, or systems only because they would be inconvenient, time-consuming or impose some cost. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

### ***Type of practices, procedures and systems***

The specific practices, procedures, and systems an agency introduces to comply with the QPPs will vary from agency to agency, however at a minimum, agencies should implement:

- procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification
- security systems for protecting personal information from misuse, interference, and loss and from unauthorised access, modification, or disclosure in accordance with QPP 11<sup>4</sup>
- a commitment to conducting a Privacy Impact Assessment (PIA) for new projects in which personal information will be handled, or when a change is proposed to information handling practices. Whether a PIA is appropriate will depend on a project's size, complexity and scope, and the extent to which personal information will be collected, used or disclosed
- procedures for identifying and responding to privacy breaches, of the QPPs including meeting any notification obligations
- clear privacy complaint procedures that explain how to make a privacy complaint and how privacy complaints or inquiries will be handled
- procedures that give individuals the option of not identifying themselves, or using a pseudonym, when dealing with the agency where doing so is practicable or permitted in accordance with QPP 2<sup>5</sup>
- governance mechanisms to ensure compliance with the QPPs, e.g., designated privacy officers and regular reporting to the agency's executive officers
- regular staff training and information bulletins on the QPPs and its QPP compliance practices, procedures, and systems

<sup>4</sup> See QPP 11 – Security, of personal information

<sup>5</sup> See QPP 2 – *Dealing anonymously or pseudonymously with an agency.*



- appropriate supervision of staff who regularly handle personal information, and reinforcement of the agency's QPP compliance practices, procedures and systems
- mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the agency comply with the QPPs. The IP Acts mandatory data breach notification rules do not apply to contractors; however, agencies should consider including data breach notification requirements in the service arrangement, e.g., that the agency and/or affected individual must be notified. Refer to **Guideline Binding contractors to the IP Act**.
- a program of proactive review and audit of the adequacy and currency of the QPP privacy policy and of the practices, procedures and systems implemented under QPP 1.

### QPP Privacy Policies

Under QPP 1, agencies must have a clearly expressed and up-to-date QPP privacy policy that explains how it manages personal information, tailored to the specific information handling practices of the agency.

If an agency has multiple responsibilities, involving different kinds of personal information being handled by separate parts of the agency or in unique ways, the most suitable approach may be a set of privacy policies (accessible from a single location on the website) to cover the different privacy practices.

A QPP privacy policy should explain how the agency manages the personal information it collects, and the information flows associated with that personal information. This reflects the central object of QPP 1, which is to ensure that agencies manage personal information in an open and transparent manner. However, the policy is not expected to detail all the practices, procedures and systems adopted to ensure QPP compliance.

The policy should be directed to the different audiences who may consult it. Primarily this will be individuals whose personal information is, or is likely to be, collected or held by the agency. If personal information is relevant to particular classes of individuals, or if information about specific community members is handled differently, this should be explained and signposted by headings. For example, if an agency adopts different practices for handling the personal information of children or individuals with a disability, this should be made clear in the policy.

At a minimum, a QPP policy should be:

- accessible
- easy to understand, avoiding or defining agency or sector specific terms, jargon, or legalistic language
- easy to find, use, and navigate; and
- only include information that is relevant to the agency's management of personal information.



There is no required style or format for a QPP privacy policy, but because it will generally be made available on the agency's website, it should be written in a way suitable for web publication.

### ***Specific information to include in a QPP Privacy Policy***

QPP 1.4 specifies the minimum information a QPP privacy policy must include:

- the kinds of personal information the agency collects and holds, including whether it collects and holds sensitive information
- how personal information is collected and held, including how the agency stores and secures personal information
- the purposes for which personal information is collected, held, used and disclosed
- how an individual can access their personal information and seek its amendment – this could include whether administrative access is available for accessing personal information and a link to the agency's RTI page
- how an individual can complain if the agency breaches the QPPs or a QPP code and how the complaint will be handled – this could refer and link to a separate privacy complaint handling procedure
- if the agency is likely to disclose personal information to overseas recipients, and, if practicable, the countries in which such recipients are likely to be located.

#### **Transparency and feedback**

A simple way of increasing transparency and evaluating the policy's effectiveness is including:

- the date it was last reviewed and/or updated; and
- contact details to which feedback on the policy can be sent, along with information about how the feedback will be handled.

### ***Data breach policies***

Under section 73 of the IP Act, agencies must publish a data breach policy. Agencies should cross-reference the QPP privacy policy and the data breach policy to improve transparency.

Refer to ***MNDB data breach register and policies*** for more information.

### ***Made appropriately available at no cost***



Agencies must take reasonable steps to make their QPP privacy policies available free of charge in an appropriate form. However, there will rarely, if ever, be no reasonable steps an agency can take to meet these obligations.

The agency's QPP Policy should be published on the agency's website, preferably linked from the website's footer, and locatable using the website's search function. The policy should meet website accessibility requirements, e.g., be compatible with screen readers.

QPP privacy policies written for online publication may be more effective and easier to understand if they use a layered approach. This involves providing a summary of key information with direct links to the policy's detailed information.

If the privacy policy is spread across multiple webpages, a PDF or link to a page containing the full policy should be included, to assist with printing and downloading.

It is important that an agency's QPP privacy policy is also available offline for no charge, e.g., a hard copy can be requested to be sent by post or made available for collection from a public facing office of the agency.

### ***Regular review***

Agencies should regularly review and update their QPP privacy policy to ensure that it reflects current information handling practices. This review could, at a minimum, be undertaken as part of an agency's annual planning processes or whenever the structure, organisation, or responsibilities of the agency change.

**For additional IPOLA assistance, please contact the IPOLA team by  
email [IPOLA.Project@oic.qld.gov.au](mailto: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](mailto:enquiries@oic.qld.gov.au)**

*Published 12 June 2024 and Last Updated 30 May 2024*