

---

## IPOLA GUIDELINE

### Basic guide to the changes in the *Information Privacy Act 2009*

**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.**

The *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (**IPOLA**) will make significant changes to the *Information Privacy Act 2009* (Qld) (IP Act) and *Right to Information Act 2009* (Qld) (**RTI Act**).

This guideline provides an overview of the changes to the IP Act. These changes will not come into effect until 1 July 2025. They are not current law.

### Definitions

There are a number of changes to definitions in the IP Act which affect the operation of the act for agencies. Some of the key definitions that are changing include:

#### Amended definitions

- personal information

#### New definitions

- affected individual
- data breach
- eligible data breach
- permitted general situations
- permitted health situations

### Access and amendment changes

IPOLA will remove access and amendment applications from the IP Act. Applications for access to documents of an agency,<sup>1</sup> even when every document

---

<sup>1</sup> Agency includes a Minister unless otherwise specified.

contains the applicant's personal information, will be made under the RTI Act. All applications to amend personal information contained in agency documents will be made under the RTI Act.

There will continue to be no application fee for amendment applications or for access applications limited to documents containing the applicant's personal information.

Refer to [Basic guide to the RTI changes](#) for more information and a provision comparison table.

## Privacy principle changes

The Information Privacy Principles (**IPPs**), which apply to non-health agencies, and National Privacy Principles (**NPPs**), which apply to health agencies, will be replaced by the Queensland Privacy Principles (**QPPs**). The QPPs will apply to every agency within the jurisdiction of the IP Act. There has been no change to the agencies which are within the jurisdiction of the IP Act.

A comparison table with more information about the privacy principles appears at the end of the guideline.

Importantly for agencies who previously need to comply with the IPPs, there is no longer a requirement for personal information to be recorded in a document for the personal information to be subject to the privacy principles.

Section 33, which currently regulates any transfer overseas of personal information, will only apply to disclosure<sup>2</sup> of personal information out of Australia.

## Mandatory Data Breach Notification

IPOLA will introduce a Mandatory Notification Data Breach (**MNDB**) scheme in Chapter 3A of the IP Act. The scheme is anticipated to commence on 1 July 2025 for all agencies other than local government. The MNDB scheme will not apply to local governments until 12 months after the scheme has commenced, anticipated commencement for local government being 1 July 2026.

The MNDB will require agencies to notify the OIC<sup>3</sup> and affected individuals<sup>4</sup> of eligible data breaches unless one of the exemptions applies<sup>5</sup>. It will also require agencies to take proactive steps to contain, assess and mitigate data breaches<sup>6</sup> and to keep a data breach register<sup>7</sup> and publish a data breach policy<sup>8</sup>.

<sup>2</sup> See section 23 IP Act for a definition of disclosure of personal information.

<sup>3</sup> Section 51 IP Act.

<sup>4</sup> Section 53 IP Act.

<sup>5</sup> Sections 55 – 60 IP Act.

<sup>6</sup> Section 48 IP Act.

<sup>7</sup> Section 72 IP Act.

<sup>8</sup> Section 73 IP Act.



Responsibility to comply with the MNDB scheme rests with agencies even if the personal information which is the subject to the breach is in the possession of a third party, provided the personal information is held<sup>9</sup> by the agency.

IPOLA will give the Information Commissioner additional powers to oversee and investigate the management and notification of eligible data breaches.

## Privacy complaints

IPOLA will introduce specific requirements complainants must meet when making a privacy complaint to an agency. It will also introduce the *response period*<sup>10</sup>, which is the timeframe agencies will have to resolve privacy complaints.

The response period will be 45 business days, which can be extended by requesting a further specified period from the complainant. If an agency requests an extension, it will be able to keep working on the complaint until the complainant refuses, the extension ends, or the agency receives notice that the complaint has been made to the Information Commissioner.

## QPP codes and Guidelines

The Minister will have the power to endorse QPP Codes and Guidelines for approval by Regulation.<sup>11</sup>

QPP Codes can state how the QPPs are to be applied or complied with and/or impose additional QPP requirements. QPP Codes will not replace the ability of the Commissioner to waive or modify the application of the privacy principles.

The Information Commissioner may prepare a guideline about the collection, use or disclosure of personal information to assist an entity locate a person who has been reported as missing and seek the endorsement of the guideline by the Minister. Approved guidelines are to be published on the OIC's website.

## QPP comparison tables

The QPPs are based on, and use the numbering of, the Australian Privacy Principles (**APPs**) in the *Privacy Act 1988* (Cth). Some APPs were not adopted, which means there are several blank QPPs.

This table sets out the QPPs and what they will cover, along with their equivalent IPPs and NPPs. In many instances, the QPPs will add to or alter the equivalent IPP or NPP<sup>12</sup>.

<sup>9</sup> Section 13 IP Act – information is held by an entity where it is contained in a document and in the possession or under the control of the entity.

<sup>10</sup> Section 164A IP Act.

<sup>11</sup> Chapter 3 IP Act.

<sup>12</sup> The use of the “+” symbol in this chart denotes a significant change to an existing IPP or NPP.



QPP	QPP requirements	IPP	NPP
1	<p>Implement practices, procedures and systems to comply with the QPPs and deal with privacy enquiries/complaints.</p> <p>Have a QPP Privacy policy that meets the listed requirements.</p>	5 +	5 +
2	<p>Allow individuals to interact anonymously or pseudonymously unless it is impracticable, or is inconsistent with an Australian law, or a court or tribunal order.</p>	-	8
3	<p>Personal information can only be collected if it is reasonably necessary for, or directly related to, one or more of the agency's functions or activities.</p> <p>Personal information which is sensitive information (defined in schedule 5) can only be collected if the agency also has consent or one of the situations in QPP 3.4 applies.</p> <p>Only applies to solicited information.</p>	1+, 3	2, 9
4	<p>Unsolicited personal information must be assessed and dealt with as set out in QPP 4.</p>	-	-
5	<p>Agency must take reasonable steps to inform individual or to ensure they are aware of the matters listed in QPP 5.2 (the QPP 5 matters).</p> <p>Applies regardless of whether information was collected from the individual or from someone else.</p>	2	1
6	<p>Personal information can be used or disclosed for the primary purpose of collection, i.e. why the agency collected it.</p> <p>It can be used or disclosed for any of the secondary purposes listed in QPP 6, which includes all the situations listed in IPP 10 &amp; 11 and NPP 2.</p> <p>See the below table for more information.</p>	10, 11	2
10	<p>Take reasonable steps to ensure personal information which is collected, used and disclosed is accurate, up to date, complete and, for use or disclosure, relevant to the purpose.</p>	3, 8, 9	3



QPP	QPP requirements	IPP	NPP
11	Take reasonable steps to protect personal information and to destroy or de-identify it once it is no longer required, unless it is part of a public record, or it is required to be kept under an Australian law, or court or tribunal order.	4	4
12	An individual can access their personal information	6	6
13	An individual can correct their personal information.	7	7

## Use and disclosure of personal information

QPP 6 will list the secondary purposes for which personal information can be used and disclosed. This will include the Permitted General Situations (**PGS**) in schedule 4, part 1 of the IP Act and, for health agencies and health information only, the Permitted Health Situations (**PHS**) in schedule 4, part 2 of the IP Act.

QPP 6		IPP	NPP
6.1	Personal information must not be used or disclosed for a secondary purpose (i.e. a purpose other than the primary purpose of collection) unless:	IPP 10, IPP 11	NPP 2
6.1(a)	The individual consents to the use/disclosure.	IPP 10(1)(a), IPP 11(b)	NPP 2(1)(b)
6.2(a)(i)	For sensitive information: the individual would reasonably expect use/disclosure for the secondary purpose and the secondary purpose is directly related to the primary purpose.	-	NPP 2(1)(a)
6.2(a)(ii)	For personal information generally: the individual would reasonably expect use/disclosure for the secondary purpose and the secondary purpose is related to the primary purpose.	IPP 10(1)(e)	NPP 2(1)(a)



QPP 6		IPP	NPP
6.2(b)	Use/disclosure is required or authorised by or under an Australian law or a court or tribunal order	IPP 10(1)(c), IPP 11(1)(d)	NPP 2(1)(f)
6.2(c), PGS 1(a)	It is unreasonable or impracticable to obtain consent and the use/disclosure is necessary to lessen or prevent a serious threat to an individual or the public.	IPP 10(1)(b), IPP 11(1)(c)	NPP 2(1)(d)
6.2(c), PGS 1(b)	There is reason to suspect unlawful activity or serious misconduct has been, is being, or may be engaged in and the agency reasonably believes use/disclosure is necessary to take appropriate action.	-	NPP 2(1)(e)
6.2(c), PGS 1(c)	Use/disclosure is reasonably necessary to assist an entity to locate a missing person and the use/disclosure is done in compliance with any Commissioner guidelines.	-	-
6.2(d), PGS 1(d)	Use/disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim	-	-
6.2(c), PGS 1(e)	The use/disclosure is reasonably necessary for a confidential ADR process.	-	-
6.2(d), PHS 4	Use/disclosure by a health agency of health information is necessary for research or compilation of statistics relevant to public health/safety.	-	NPP 2(1)(c),
6.2(d), PHS 5	Disclosure of health information by a health agency	-	NPP 2(3), NPP 2(4)



QPP 6		IPP	NPP
	to a person responsible for an individual.		
6.2(e)	The agency reasonably believes use/disclosure is necessary for an enforcement related activity conducted by or on behalf of a law enforcement agency.	IPP 10(1)(d), IPP 11(1)(e)	NPP 2(1)(g)
6.2(f)	Disclosure to ASIO.	IPP 11(1)(ea)	-
6.2(g)	Use/disclosure for public interest research and/or the compilation of statistics.	IPP 10(1)(f), IPP 11(1)(f)	-
6.4	Health agency pre-disclosure de-identification obligations for personal information collected under schedule 4, part 2, section 3.	-	NPP 9(4)
6.5	The agency must make a written note of any use or disclosure under 6.2(e).	IPP 11(2)	NPP 2(2)

**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)**

*Last Updated and published on 28 May 2024.*