# Policy

## I27 QPP privacy policy

### Purpose

The *Information Privacy Act 2009* (Qld) (IP Act) and Queensland Privacy Principles (QPPs) govern how the Queensland public sector handles personal information.

This policy outlines how QAO manages personal information, including:

- the types of personal information we collect, hold, use and disclose
- how we manage and respond to privacy complaints.

### Application

The policy applies to the QAO workforce, including permanent, temporary, casual, and contracted employees. It also applies to Audit Service Providers (ASPs).

This policy does not cover information requests (access requests), such requests will be dealt with under QAO policy I25 *Right to information*.

### Legislative context

- *Auditor-General Act 2009* (AG Act)
- *Information Privacy Act 2009* (IP Act)
- *Privacy Act 1988* (Cth)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)
- *Right to Information Act 2009* (RTI Act)

### Definitions/glossary of terms

| Term | Definition |
|---|---|
| **Eligible data breach** | Per s.47 of the *Information Privacy Act 2009.*<br>An *eligible data breach* of an agency is a data breach of the agency that occurs in relation to personal information held by the agency if—<br>(a) both of the following apply—<br>(i) the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information;<br>(ii) the access or disclosure is likely to result in serious harm to an individual (an ***affected individual***) to whom the personal information relates, having regard to the matters stated in subsection (2); or<br>(b) the data breach involves the personal information being lost in circumstances where—<br>(i) unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and |

| Term | Definition |
|---|---|
| | if the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual (also an affected individual) to whom the personal information relates, having regard to the matters stated in subsection (2). |
| **Personal information** | Has the meaning given in s.12 of the *Information Privacy Act 2009.*<br>Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion—<br>(a) whether the information or opinion is true or not; and<br>(b) whether the information or opinion is recorded in a material form or not. |
| **Protected information** | Has the meaning given in s.53 of the *Auditor-General Act 2009.*<br>Protected information means information, observations, comments, suggestions or notations that—<br>(a) are not publicly available; and<br>(b) are disclosed to, obtained by or made by a person to whom this section applies in relation to an audit that has been, is being or will be conducted under this Act; and<br>(c) are relevant to the audit. |
| **Sensitive information** | Has the meaning given in sch. 5 of the *Information Privacy Act 2009.*<br>Sensitive information of an individual means the following:<br>(a) information or an opinion about an individual's<br>i. racial or ethnic origin; or<br>ii. political opinions; or<br>iii. membership of a political association; or<br>iv. religious beliefs or affiliations; or<br>v. philosophical beliefs; or<br>vi. membership of a professional or trade association; or<br>vii. membership of a trade union; or<br>viii. sexual orientation or practices; or<br>ix. criminal record<br>(b) health information about an individual; or<br>(c) genetic information about an individual that is not otherwise health information; or<br>(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or<br>(e) biometric templates. |

## Policy statement

QAO will:

- comply with Queensland Privacy Principles (QPPs).
- only collect, use and store the personal information we require to perform our official duties and meet legislative obligations.
- identify, contain, investigate and respond to eligible data breaches as required under legislation.
- process privacy complaints in accordance with QAO policy I22 *Security incident, event, and breach management.*
- use threshold privacy assessments and privacy impact assessments to inform business decisions i.e., using software hosted outside of Australia.

# Principles

## Collection of personal information

We may collect personal information:

- directly from individuals who access our services or indirectly from third parties as part of carrying out our functions. This includes:
  - conducting audits under the *Auditor-General Act 2009* (AG Act)
  - assessing the suitability of individuals applying to be registered as an audit service provider
  - responding to enquiries from the public and other agencies
  - responding to public interest disclosures under the *Public Interest Disclosure Act 2010* (PID Act)
  - dealing with access applications under the *Right to Information Act 2009* (RTI Act)
  - dealing with privacy complaints or eligible data breaches under the IP Act
  - monitoring compliance with legislation, policies and procedures.
- to carry out business functions such as employee management, recruitment and selection, procurement and financial management.
- indirectly collect personal information which is recorded within an agency document obtained for the purposes of delivering our mandate under the AG Act.

We may also collect sensitive information. In the event this is required and where appropriate, we will only collect this information directly from the individual to whom it is about or with their consent.

The type of personal information we collect will vary depending on the circumstance. Examples of the types of personal information we collect, and hold are set out in the table below.

| QAO function | Kind of personal information, how and why we collect it |
|---|---|
| **Public sector audit** | We may collect personal information about persons associated with or employed by an audit client. This may include, but is not limited to names, positions, payroll records or contractual arrangements. |
| **Management of QAO workforce** | We collect personal information about individuals applying to or employed by QAO. This may include, but is not limited to names, addresses, phone numbers, dates of birth, employment history, bank account details, photograph or medical records. |
| **Operation of our financial management system** | We collect personal information when a member of the QAO workforce conducts a financial transaction on behalf of the Office e.g., use of corporate card. This may include, but is not limited to names, bank account details, residential addresses or phone numbers. |
| **Engagement/ management of audit service providers** | We collect personal information about individuals applying to be registered as an ASP. This may include, but is not limited to an auditor's name, qualifications, employment history, contact details or photograph. |
| **Administrative information** | We collect personal information pertaining to the QAO workforce, audit clients and other visitors to our office or external website, including event registration. This may include, but is not limited to names, email addresses or phone numbers. |
| **Client feedback** | We invite audit clients, audit service providers, parliamentarians and audit committee chairs to provide feedback on our products and services. Survey participants can choose whether to provide their personal information to us. |
| **Complaints** | We may collect personal information about individuals who make complaints to QAO including privacy or conduct complaints. This may include names and contact details. |

## Use and disclosure of personal information

We may use and disclose personal information for the purpose for which it was collected, including:

- delivering our audit mandate under the AG Act
- managing associated business processes, such as recruitment and human resources administration.

We may also use or disclose personal information for secondary or alternative purposes as permitted under the AG Act (e.g., sharing protected information with the Crime and Corruption Commission), or where we are authorised or required under Australian law.

## Access and amendment of personal information

We will deal with all requests to access or amend personal information in accordance with the RTI Act.

## Disclosure out of Australia

In the event we need to disclose personal information outside of Australia, this will occur either with consent, where we are authorised or required by law, or in accordance with the IP Act.

## Dealing with QAO anonymously or using a pseudonym

There are limited circumstances where a person may choose to deal with us anonymously or by using a pseudonym, these include:

- Contributing to an audit
- Suggesting an audit topic
- Raising an issue about financial waste or mismanagement
- Making a complaint about QAO
- Making an enquiry.

Importantly, depending on the nature of the interaction, we may not be able to action a complaint and/ or provide a response without a person's identity.

Anonymous or pseudonymous interaction is not possible for any other QAO function.

## Security of personal information

We will handle personal information in a secure manner and take all reasonable steps to protect it from misuse, interference, loss, unauthorised access, modification or disclosure.

We comply with relevant Queensland Government information standards and security protocols.

Where permitted we will destroy or de-identify unsolicited personal information in accordance with our obligations under the QPPs and if it is lawful and reasonable to do so.

## Privacy complaints

Individuals who feel their personal information has been mishandled may lodge a privacy complaint with QAO. The complaint may also be lodged by an authorised representative on behalf of the affected party but only where the person:

- consents; or
- is a child/ minor and the complaint is being lodged by their parent or guardian;
- lacks capacity and the complaint is being lodged by their guardian; or

- has a legal authority to act on behalf of the affected party.

Privacy complaints must be:

- made in writing and include:
  - an address for us to respond to you (e.g., an email address)
  - details about the matter or issues you are complaining about (e.g., what did the QAO do or not do with your personal information that you believe breached the QPPs and the IP Act).
- lodged within 12 months of becoming aware of the act or practice you think constitutes a breach by QAO of the IP Act.

Where a privacy complaint is made by another person, then the complaint should be supported by sufficient evidence to show that they have authority to act on behalf of the affected person.

### *Contact details for privacy complaints*

**Email**: qao@qao.qld.gov.au

**Post**: PO Box 15396, City East, Qld 4002

### *Handling privacy complaints*

Privacy complaints will be dealt with by independent officers and resolved within 45 business days.

If a complainant is dissatisfied with our response, then a complaint can be lodged with the Office of the Information Commissioner (OIC) in accordance with their *Make a privacy complaint procedure,* available from: *https://www.oic.qld.gov.au/about/privacy/make-a-privacy-complaint-2*.

## Last approved: 12 August 2025