



# Privacy plan

---

# Contents

---

<b>Introduction</b>	<b>1</b>
What is personal information?	1
Other legislation	1
<b>Our work</b>	<b>2</b>
Our workforce	2
Privacy complaints	2
<b>Types of personal information</b>	<b>3</b>
<b>Accessing personal information</b>	<b>4</b>
Request to access personal information	4
Request to amend personal information	4
<b>A. Auditor-General Act 2009</b>	<b>5</b>

# Introduction

---

The *Information Privacy Act 2009* (IP Act) regulates how Queensland Government departments, Ministers, local governments and public authorities, such as the Queensland Audit Office (QAO), manage personal information. It creates an obligation to comply with the privacy principles and affords individuals the right to access and amend their personal information.

The eleven Information Privacy Principles (IPPs) apply to us and specify how we collect, store, secure, access, amend, use and disclose personal information.

## What is personal information?

The IP Act defines personal information as ‘information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.’

For the purposes of this plan, personal information is defined as any information that could identify or reveal the identity of another person. The information does not have to clearly identify the person but need only provide sufficient information to lead to the identification of the person. Examples of personal information include, but are not limited to, a person’s name or a photograph of a person.

## Other legislation

### Auditor-General Act 2009

The *Auditor-General Act 2009* (AG Act) provides the legal basis for the Auditor-General’s access to all government information and for the Auditor-General to conduct audits in any way considered appropriate and without direction by any person. Section 53 defines the confidentiality provisions applicable to protected information, and identifies the situations where it is permissible for a person, subject to the confidentiality provisions, to disclose protected information – refer to appendix A.

### Right to Information Act – exempt information

The *Right to Information Act 2009* (RTI Act) provides members of the public with a right to access information in the government’s possession or under the government’s control unless, on balance, it is contrary to the public interest. Schedule 3 of the RTI Act sets out the types of information the disclosure of which the Parliament considers would, on balance, be contrary to the public interest.

Section 12(1) describes the category of information deemed to be exempt information on the basis, *disclosure is prohibited by a legislative provision*.

The confidentiality provisions of the AG Act are recognised as provisions prohibiting disclosure, and any request to access protected information, specifically where it contains personal information, would be carefully considered to ensure disclosure was in the public interest.



# Our work

---

We are Queensland's independent auditor of state and local government public sector entities, as established under the AG Act. Our role is to provide independent assurance to the people of Queensland on the financial management and performance of public sector entities.

We achieve this by:

- providing professional audit services, which include our audit opinions on the accuracy and reliability of the financial statements of public sector entities and local governments
- providing entities with insights on their financial performance, risk, and internal controls; and on the efficiency, effectiveness, or economy of public service delivery
- produce reports to parliament on the results of our audit work, our insights and advice, and recommendations for improvement
- conduct investigations about financial waste and mismanagement raised by elected members, state and local government employees and the general public
- share the wider learnings and best practice, from our work, with state and local government entities, and our professional networks, industry, and peers.

## Our workforce

Our workforce includes permanent, temporary and casual employees, contractors, and Audit Service Providers (ASPs). ASPs are external audit firms engaged to conduct audits on behalf of the Auditor-General.

Our workforce is responsible for managing personal information in accordance with the RTI and IP Acts and this privacy plan. They are also subject to the confidentiality provisions of the AG Act which prohibits the disclosure of protected information. We educate our workforce about the IP Act and Information Privacy Principles (IPPs) through our onboarding process, the provision of compulsory online training and the use of specific contract conditions for our ASPs.

## Employees and contractors

We have strict security protocols in place for the management of our information and ICT devices, and all employees and contractors are required to sign a confidentiality agreement upon commencement with the Office. We also only give people access to information that is necessary to fulfil their duties.

## Audit Service Providers

Where an ASP collects, accesses, uses or stores personal information in order to perform auditing services, they must comply with the IPPs as stipulated in the IP Act.

## Privacy complaints

If you believe that QAO has not dealt with your personal information in accordance with the IP Act, you may make a written complaint. Complaints can be lodged in person, post or via email.

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

**In person**—Level 13, 53 Albert Street Brisbane 4001

**Email**—[qao@qao.qld.gov.au](mailto:qao@qao.qld.gov.au)

We will process privacy complaints in accordance with our Complaints Handling Policy.



# Types of personal information

We deal with the following types of personal information:

Type of personal information	Collect	Use	Store	Disclose
Engagement/ management of Audit Service Provider (ASP)	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.	We may use the personal information to: <ul style="list-style-type: none"> <li>• help assess the performance of an ASP, including quality assurance reviews</li> <li>• assess the suitability of applicants for registration or appointment as an ASP</li> <li>• raise awareness for technical or professional development opportunities relevant or of interest to the ASP.</li> </ul> Delegated officers may amend personal information at the request of an individual or management.	We will: <ul style="list-style-type: none"> <li>• store the personal information in a format suitable for our business needs e.g. physical or digital</li> <li>• apply a security classification and ensure appropriate controls are in place to protect the information from inappropriate use or disclosure</li> <li>• grant officers access to the personal information based on the need-to-know principle</li> <li>• retain contractual records in accordance with an approved retention and disposal schedule.</li> </ul>	We may disclose contractual information in our annual report, but we will not disclose personal information to other people or organisations without consent from the person to which the information relates, unless there is a statutory or contractual arrangement in place.
Conduct of a 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, residential addresses, job positions, payroll records or contractual arrangements.	We may use the personal information to: <ul style="list-style-type: none"> <li>• assist in the provision of audit and assurance services</li> <li>• act as audit evidence to support a decision or judgment</li> <li>• raise awareness for technical or professional development opportunities relevant to or of interest to the audit client or their associates.</li> </ul>	We will: <ul style="list-style-type: none"> <li>• store the personal information in a format suitable for our business needs</li> <li>• apply a security classification and ensure appropriate controls are in place to protect the information from inappropriate use or disclosure</li> <li>• restrict access to our audit and assurance files to only the assigned audit team and our quality assurance reviewers</li> <li>• grant officers access to the personal information based on the need-to-know principle, and after consideration of their independence declarations</li> <li>• retain audit records in accordance with an approved retention and disposal schedule.</li> </ul>	We will not disclose any information created or obtained during the course of an audit except in accordance with the confidentiality provisions of the AG Act.
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 i.e. use of corporate card. This may include, but is not limited to: names, bank account details, residential addresses or phone numbers.	We may use the personal information to process or reconcile corporate expenditure records	We will: <ul style="list-style-type: none"> <li>• store the personal information in a format suitable for our business needs e.g. physical or digital</li> <li>• apply a security classification and ensure appropriate system controls are in place to protect the information from inappropriate use or disclosure</li> <li>• grant officers access to the personal information based on the need-to-know principle</li> <li>• retain financial records in accordance with an approved retention and disposal schedule.</li> </ul>	We may disclose this type of information to our auditors, but we will not publicly disclose this information unless it relates to overseas travel or gifts and benefits. Information about overseas travel and gifts and benefits received by the QAO workforce are published on our external website.
Management of QAO employees	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 or medical records.	We may use the personal information to: <ul style="list-style-type: none"> <li>• maintain an employment history for current and former members of the QAO workforce</li> <li>• assess the suitability of applicants/employees to perform the duties associated with particular positions</li> <li>• facilitate the payment of salaries and wages and other benefits/reimbursements</li> <li>• assess an employee's compliance with corporate policies and procedures.</li> </ul> Delegated officers may amend personal information at the request of an individual or management.	We will: <ul style="list-style-type: none"> <li>• store the personal information in a format suitable for our business needs e.g. physical or digital</li> <li>• apply a security classification and ensure appropriate controls are in place to protect the information from inappropriate use or disclosure</li> <li>• grant officers access to the personal information based on the need-to-know principle</li> <li>• retain records in accordance with an approved retention and disposal schedule.</li> </ul>	We may disclose personal information to a third party, such as the Australian Taxation Office, in the interest of fulfilling our roles and responsibilities as an employer.
Administrative information	We collect personal information pertaining to the QAO workforce, audit clients and other visitors to our office or external website.	We may use the personal information to: <ul style="list-style-type: none"> <li>• facilitate the operation of support services, which may include but is not limited to correspondence, policies, mailing lists, publications, email communications and internal announcements</li> <li>• aid in the detection of security breaches or employee misconduct through the use of closed circuit television (CCTV) system</li> <li>• act as evidentiary material in the event a criminal offence or security breach is detected.</li> </ul> Delegated officers may amend personal information at the request of an individual or management.	We will: <ul style="list-style-type: none"> <li>• store the personal information in a format suitable for our business needs e.g. physical or digital</li> <li>• apply a security classification and ensure appropriate controls are in place to protect the information from inappropriate use or disclosure</li> <li>• grant officers access to the personal information based on the need-to-know principle</li> <li>• store CCTV footage in a secure location</li> <li>• retain records in accordance with an approved retention and disposal schedule.</li> </ul>	We may provide copies of personal information to a law enforcement agency in the event a criminal investigation or in the event of employee misconduct.



# Accessing personal information

---

## Request to access personal information

Under the IP Act, a person or their agent can apply to the QAO to seek access to personal information in our possession or control.

To request access, you must:

- lodge a completed [RTI and IP Access Application](#)
- provide enough information to identify the document/s
- provide an address (post or email)
- provide evidence of your identity
- provide evidence of the agent's authorisation and their identity, if necessary.

## Request to amend personal information

Under the IP Act, a person can apply to the QAO to have their personal information amended if it is inaccurate, incomplete, out-of-date or misleading.

To apply for amendment, you must:

- have seen the document or have a copy of it
- provide enough information to identify the document
- provide an address (post or email)
- specify the information you want amended
- explain how the information is inaccurate, incomplete, out-of-date or misleading
- suggest how you want the information changed
- lodge a completed [IP Personal Information Amendment Application Form](#)
- provide evidence of your identity.

## Lodging applications

The QAO can accept completed applications in the following ways:

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

**In person**—Level 13, 53 Albert Street Brisbane 4001

**Email**—[qao@qao.qld.gov.au](mailto:qao@qao.qld.gov.au)



# A. Auditor-General Act 2009

---

## 53 Confidentiality and related matters

- 1) This section applies to a person who is or has been any of the following, including before the commencement of this subsection—
  - a. an authorised auditor;
  - b. a person engaged by the auditor-general;
  - c. a person engaged or employed by a contract auditor;
  - d. a person receiving proposed reports, or extracts of proposed reports, under [section 64](#).
- 2) The person must not—
  - a. make a record of protected information; or
  - b. whether directly or indirectly, divulge or communicate protected information;

unless the record is made, or the protected information is divulged or communicated, under this Act or in the performance of duties, as a person to whom this section applies, under this Act.

Maximum penalty—200 penalty units or imprisonment for 1 year.
- 3) Subsection (2) does not prevent the disclosure of protected information to—
  - a. the parliamentary committee or a portfolio committee; or
  - b. the Crime and Corruption Commission; or
  - c. a police officer, or an entity, responsible for the investigation or prosecution of offences in any jurisdiction; or
  - d. a court for the purposes of the prosecution of a person for an offence in any jurisdiction; or
  - e. if the auditor-general conducts an audit jointly, or in collaboration, with the auditor-general of the Commonwealth or another State under [section 42A](#)—the auditor-general of the Commonwealth or other State; or
  - f. the Treasurer or the department in which the [Financial Accountability Act 2009](#) is administered.
- 4) Compliance by a person mentioned in subsection (1) in relation to the Corporations Act, section 311 or the *Australian Securities and Investments Commission Act 2001*, section 30A is declared to be an excluded matter for the Corporations Act, section 5F.
- 5) Nothing in subsection (4) is intended to affect the power of a person mentioned in subsection (1) to disclose information to the Australian Securities and Investments Commission under subsection (3)(c).
- 6) In this section—
 

**protected information** means information, observations, comments, suggestions or notations that—

  - a. are not publicly available; and
  - 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
  - c. are relevant to the audit.



[qao.qld.gov.au](http://qao.qld.gov.au)

---



- [Suggest a performance audit topic](#)
- [Contribute to a performance audit in progress](#)
- [Subscribe to news](#)
- [Connect with QAO on LinkedIn](#)

T: (07) 3149 6000  
E: [qao@qao.qld.gov.au](mailto:qao@qao.qld.gov.au)  
W: [qao.qld.gov.au](http://qao.qld.gov.au)  
53 Albert Street, Brisbane Qld 4000  
PO Box 15396, City East Qld 4002

 **Queensland  
Audit Office**  
*Better public services*

