

Policy number	GOV-005 2024 PR1
eDocs	239704
Type	Procedure
Status	Final
Classification	Public

# QPP Privacy Policy

Version: 3 | Date effective: 1 July 2025 | Review date: 1 July 2026

## Audience

All staff, including contractors and volunteers.

## Purpose

The *Information Privacy Act 2009* (IP Act) regulates how public sector agencies and statutory bodies, such as the Office, manage personal information. It creates an obligation to comply with the Queensland Privacy Principles (QPPs) which are contained in Schedule 3 to the IP Act.

This policy sets out how the Office collects, manages, uses and discloses personal information in compliance with the IP Act and QPPs.

## Application

This policy applies in relation to all documents of the Office that may contain personal information.

## Responsibilities

Officer	Responsibilities
General Counsel	<ul style="list-style-type: none"> <li>Provide legal advice to the Office on the application and implementation of the IP Act and the QPPs</li> <li>Provide advice and support to the Advisor RTI/IP in managing privacy complaints</li> </ul>
Advisor, RTI/IP	<ul style="list-style-type: none"> <li>Undertake privacy breach assessments</li> <li>Manage privacy complaints</li> <li>Undertake privacy impact assessments</li> <li>Undertake periodic privacy audits</li> <li>Provide advice and training to staff</li> </ul>
All employees	<ul style="list-style-type: none"> <li>Manage personal information in accordance with the QPPs</li> </ul>

---

## Requirements *Collection of personal information*

The definition of 'personal information' is set out in the 'Definitions' on page 8.

The Office has powers under the *Ombudsman Act 2001* and the *Inspector of Detention Services Act 2022* to collect information, which may include personal information, and to use this information for certain purposes. The Ombudsman is also the oversight agency for the *Public Interest Disclosure Act 2010 (PID Act)*.

In addition, the Office is empowered under legislation to collect information, including personal information, for the purposes of recruitment, selection and employment of officers, and the engagement of contractors.

We collect personal information directly from individuals who access our services and indirectly from third parties as part of carrying out our functions.

The categories of information collected encompass records kept by the Office in accordance with the *Public Records Act 2023* and information received from external agencies and individuals:

- complaint information
- information collected during a review of a detention service or an inspection of a place of detention
- survey information
- employee and recruitment information
- trainee information
- supplier information
- information in public reports
- subscriber list information
- cookies and website analytics.

Information is collected in various ways including:

- notes taken during telephone calls, interviews and from recorded voice messages
- notes taken during a review of detention services and inspections of places of detention
- minutes of meetings
- online complaint and contact forms submitted through the website
- training booking forms
- emails, voicemail, Teams and text messages,
- mail, including letters and other documents
- CDs, USB drives, links to shared cloud drives and other recordings
- approved access to other agency information, for example via databases

In accordance with the *Records management policy*, all officers receiving information or recording information are responsible for entering that information in the Office's recordkeeping systems.

### ***Sensitive information***

We may also collect sensitive information. The definition of 'sensitive information' is set out in the 'Definitions' on page 9. We will generally only collect sensitive information directly from the individual it is about or with their consent, or otherwise consistently with our obligations under the IP Act.

### ***Anonymity and pseudonymity***

Individuals have the option of dealing with the QO anonymously. This means that the individual does not need to provide personal information or information that might identify them.

Individuals may also provide a pseudonym, this means giving the QO a name, term or descriptor instead of their actual name.

Where an individual chooses to remain anonymous or use a pseudonym, the QO may not be able to provide some services, for example, we may not be able to investigate a complaint, follow up with another agency or provide feedback.

### ***Holding personal information***

The Office holds personal information in multiple physical and electronic locations:

- electronic document and records management system (eDOCS) for general administrative documents
- electronic complaints management system (Resolve) for information relating to complaints
- hard copy records held in the Office, off-site storage and with State Archives
- various information technology platforms for communications, web services, social media, training services, voluntary surveys, and newsletters

In accordance with the PID Act and the *Public Interest Disclosure Standard No. 3/2019*, public sector entities are required to submit information about PIDs through the RaPID database. However, RaPID does not require personal information identifying individuals involved in a PID. Agencies are alerted to their confidentiality obligations under the PID Act when entering data.

All information is retained in accordance with the Retention and Disposal schedule approved by Queensland State Archives under the *Public Records Act 2023* and with the requirements of the Australian Taxation Office.

### **Security of personal information**

The QO holds personal information securely and takes reasonable steps to protect it from misuse, interference, loss, unauthorised access, modification or disclosure. QO complies with relevant Queensland government Information Standards and security protocols to protect personal information and ensure it can be accessed by authorised staff members only.

Where permitted by the *Public Records Act 2023* (Qld), QO will destroy or deidentify unsolicited personal information or personal information no longer required for any of its functions in accordance with our obligations under the QPPs if it is lawful and reasonable to do so.

### ***Using and disclosing personal information***

The types of personal information (including sensitive information) the Office may collect, and the ways in which that information may be used, includes:

#### **Personal information obtained in the course of receiving, assessing and responding to complaints or inquiries**

This information may comprise a wide range of personal information of any type about complainants, third parties or agency officers. It is used for:

- responding to inquiries
- assessing jurisdiction under the Ombudsman Act
- responding to complaints and conducting investigations under the Ombudsman Act

- the compilation of statistics for internal use or publication (in a de-identified form).

Any employee with responsibility for receiving, assessing, investigating, responding to, or reviewing the management of an inquiry or complaint, and their supervisors/managers, may have access to the information.

The Ombudsman Act (ss 92) restricts the disclosure of information obtained in a preliminary inquiry or investigation, or for the performance of another function of the Ombudsman, except in particular circumstances. Information may be disclosed for the performance of the Ombudsman's functions, as part of formulating reports or recommendations, and for other purposes set out in the Act.

Information may be disclosed to the agency complained about in order to obtain that agency's response to the details of the complaint or to seek clarification or further information. Information may also be disclosed to another agency where the Ombudsman considers the agency has a proper interest in the information for the purpose of its functions, or if the disclosure is for the purpose of protecting the health, safety or security of a person or property.

This information may, with the complainant's consent (where it is reasonably able to be obtained), be referred to another agency to deal with where necessary or appropriate.

In some cases, we are required by law to notify another agency of a matter, and consent is not required (for example, notification to the Crime and Corruption Commission of corrupt conduct).

#### **Personal information obtained in the course of carrying out a review or inspection of a detention service**

This information may include a wide range of personal information of any type about detainees, third parties or agency officers. It is used for:

- carrying out a review or inspection of a detention service under the IDS Act; and
- reporting to the Legislative Assembly (and to the public) on reviews and inspections, including formulating advice and recommendations in these reports; and
- other purposes as set out in the IDS Act.

The Inspector, and any employee responsible for collecting information, engaging with detainees, organising information, researching, conducting or analysing data and findings from a review or inspection, and their supervisors/manager, may have access to this type of information.

While personal information may be collected during inspections and reviews, and it may inform reports and recommendations, the Inspector will not ordinarily include the personal information of detainees in reports.

The IDS Act (Part 4, Division 2) prohibits the disclosure or use of confidential information (which captures personal information), except in certain circumstances. Personal information may also be used/disclosed for:

- performing functions under the Act (for example, formulating recommendations about taking action to promote improvement of detention services)
- seeking help from a suitable person to carry out a review or inspection under s 9 of the IDS Act
- consulting with or engaging people with skills, expertise or experience to help carry out the Inspector's functions
- sending show cause notices to the responsible officer for a place of detention and referring certain matters to the responsible Minister, where this is required by the IDS Act (for example, where there is a serious risk to the safety of a detainee)
- referring matters to other entities, where the matter can be more appropriately dealt with by the other entity, as set out in s 20 of the IDS Act
- disclosing information in circumstances that are in the public interest, as set out in s 31 of the IDS Act; and

- reporting annually on our operations and compiling information and statistics for internal use or publication (in a de-identified form).

At times, we may also disclose information to other entities, where this is permitted or required by law. In some cases, consent is not required ((for example, notification to the Crime and Corruption Commission of corrupt conduct).

### **Personal information collected and used in the course of conducting surveys**

Personal information may be used by the Office to conduct surveys to evaluate and improve performance, and to compile relevant statistics for internal use or publication (in a de-identified form):

- surveys of complainants about the Office's service and complaint outcomes
- surveys of internal and external officers attending training
- staff satisfaction surveys.

Complainants are given an opportunity to advise the Office that they do not wish to be surveyed. Completion of all surveys is voluntary.

Personal information (name and contact details only) may be provided to an external entity solely for the purpose of conducting surveys on behalf of the Office.

Where the Office enters into agreements with external entities to conduct surveys, the contract must include terms requiring that the contractor must:

- comply with the IP Act and
- keep all personal information confidential
- not disclose information provided by the Office, or received in the course of conducting the survey, to any person other than an employee of the Office.

### **Personal information about employees relating to human resource management functions**

Records relating to current and former employees (including casual and temporary), encompass recruitment, selection, appointment, demographic information, payroll, banking, leave, performance appraisal and other information.

Personal information collected may include name, date of birth, gender, qualifications, employment history, criminal history checks, occupation, employee identification number, next of kin, relationship details, personal financial information, salary and allowances, medical information, timesheets, leave details, overtime records, travel records, work reports, performance assessments, service and staff awards, disciplinary investigations and actions, and records of information technology system usage. Information collected may be of a highly sensitive nature, for example information relating to health, family members and children, bereavement, domestic violence, grievances, or public interest disclosures.

This information is used for internal human resource management functions and contributes to protecting and maintaining computer and network system performance and security.

Limited and specific personal information is disclosed to third parties to fulfill those functions (for example, external payroll providers, Q-Super, the Australian Taxation Office, organisations in receipt of payroll deductions). In certain circumstances personal information about employees may be disclosed to external medical/emergency personnel.

Recruitment records may consist of applications for employment, interview notes, selection panel assessments, criminal history checks, serious disciplinary history checks, referee checks and correspondence to unsuccessful and successful candidates.

This information is collected and used solely for the purpose of selecting employees. It may be accessed by employees (or external officers) appointed to sit on selection panels, the delegate responsible for approving appointments, and any employee assisting with the administrative functions associated with recruitment.

Relevant information from an applicant's application may be disclosed to nominated referee/s in the course of conducting referee checks. De-identified information about the selection panel's assessment of the successful applicant may be disclosed to other applicants as part of a feedback process, but otherwise, this information is not further disclosed without the consent of the individual.

Internal communications may be monitored by information technology staff for system troubleshooting, maintenance and security purposes.

Internal and external auditors may access any and all information held by the Office relevant to the conduct of an audit.

Otherwise, information is only disclosed to third parties with the permission of the employee or as required by law (for example, to the Crime and Corruption Commission in connection with allegations of corruption).

### **Translation and interpreting services**

The QO may provide information to a translation service where correspondence is received in a language other than English. We may also use an interpreting service to communicate with individuals in their own language.

### **Legal services**

The QO may provide information to a legal representative for the purpose of seeking legal advice in relation to any matter. This communication is subject to legal professional privilege and is confidential.

### **Training Services**

We use an eLearning system to provide training services. Personal information collected may include a user's name, phone number, email address, username, role, where employed, course name and whether the course was completed.

This information is collected and used solely for the purpose of conducting training and enhancing and improving the training services provided by the Office, and to compile relevant statistics for internal use or publication (in a de-identified form).

### **CCTV**

Persons attending the Office's premises will be recorded by way of closed circuit television (CCTV) security system. The CCTV surveillance system is operated and managed by the Building Security Coordinator, which is part of the Queensland Police Service. CCTV images are recorded, collected, stored, monitored and reviewed for the purposes of promoting the health and safety of employees, public safety, security, crime prevention and detection.

The QO can request CCTV surveillance footage and images only in exceptional circumstances, such as the investigation of a serious employee misconduct matter.

Further information is detailed in the Office's *CCTV policy*.

### **Personal information about suppliers and potential suppliers of goods or services**

Personal information may be collected about suppliers and potential suppliers of goods or services who are trading as individuals. It may include names, contact details, bank account information and Australian Business Numbers and credit/debt information. This information is used only to facilitate the supply of, and payment for, goods and services.

### **Subscriber lists**

The Office distributes e-newsletters targeted at particular audiences, including public sector officers, community organisations, and PID coordinators. The Office may collect personal information such as name, occupation and email address. A person will only be added to a subscriber list by request.

Public sector officers who are authorised as users of the public interest reporting database (RaPID) will be automatically added to the subscriber list for the PID e-newsletter.

Subscribers can unsubscribe at any time through a e-newsletter received or by contacting the Office.

### **Public reports**

Section 92 of the Ombudsman Act restricts the disclosure of information obtained under the Act, except in certain circumstances including purposes connected with investigating complaints, helping agencies improve their administrative practice, and the publication of reports to agencies, Ministers and Parliament. This Office will not publish private complainant information in a public report without consent.

### **Cookies**

The Office's website uses cookies to collect information for statistical purposes including:

- the time and date of visit
- the website visited immediately prior
- country and city of location
- the pages and documents accessed
- users internet service provider.

### **Website analytics**

The Office uses Google Analytics on its website to gather anonymous information about visitors. When a person visits a web page their browser automatically sends anonymous information to Google. Examples of the information include the web address of the page visited, the person's IP address and demographic information. Google may also use cookies.

The Office uses this data to analyse the pages that are visited, to improve user experience and the website.

A person can choose not to allow Google to collect their information by opting out of Google Analytics or specifically opting out of Google Analytics display advertiser features.

### **Social media platforms**

This office uses social media platforms to communicate with the public and to raise awareness of our services. When individuals communicate with us via these social media platforms, we collect any personal information provided to us.

### **Disclosure outside of Australia**

We would generally disclose personal information overseas only when necessary to address a complaint or inquiry within our statutory functions and obligations. For instance, where a complainant is overseas.

We use various information technology providers for communications, web services, social media, training services, voluntary surveys, and newsletters. These providers may collect and hold your personal information overseas.

Where we disclose personal information overseas, this will usually occur with agreement, where we are authorised or required by law, or otherwise consistently with our obligations under the IP Act.

### ***Third party service providers***

If the Office enters into a contract or other arrangement for the provision of services associated with the performance of any of the Office's functions, the Office will take all reasonable steps to ensure that the service provider is required, in discharging its obligations under the contract or arrangement, to comply with the relevant obligations contained in the IP Act, as if it were the Office.

The Office must ensure that the contract or arrangement contains appropriate privacy clauses that require the contractor to comply with the Information Privacy Act.

### ***Accessing or amending personal information***

Under the IP Act a person may apply to access or amend their personal information held by the Office. The process for making an application and responding to it is set out in the Office's *Access to and amendment of information policy and Access to and amendment of information procedure*.

### ***How to complain about a breach of privacy***

How to complain about a breach of privacy and how the Office deals with privacy complaints is set out in the *Data and Privacy Breach Policy* and the *Privacy Complaint Procedure*.

## **Definitions**

<b>Term / Acronym</b>	<b>Definition</b>
<b>Advisor, RTI/IP</b>	Advisor, Right to Information and Privacy
<b>GRDS</b>	General Retention and Disposal Schedule
<b>IDS Act</b>	<i>Inspector of Detention Services Act 2022</i>
<b>IP</b>	Information Privacy
<b>IP Act</b>	<i>Information Privacy Act 2009</i>
<b>Office</b>	Office of the Queensland Ombudsman
<b>Ombudsman</b>	Queensland Ombudsman and Inspector of Detention Services
<b>Personal information</b>	<p><b>Personal information</b> means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion—</p> <ul style="list-style-type: none"> <li>(a) whether the information or opinion is true or not; and</li> <li>(b) whether the information or opinion is recorded in a material form or not.</li> </ul> <p>(Section 12 of the IP Act)</p>

<b>Sensitive information</b>	<p><b>Sensitive information</b> for an individual, means the following:</p> <p>(c) information or an opinion about an individual's:</p> <ul style="list-style-type: none"> <li>(i) racial or ethnic origin; or</li> <li>(ii) political opinions; or</li> <li>(iii) membership of a political association; or</li> <li>(iv) religious beliefs or affiliations; or</li> <li>(v) philosophical beliefs; or</li> <li>(vi) membership of a professional or trade association; or</li> <li>(vii) membership of a trade union; or</li> <li>(viii) sexual orientation or practices; or</li> <li>(ix) criminal record;</li> </ul> <p>(d) health information about an individual; or</p> <p>(e) genetic information about an individual that is not otherwise health information; or</p> <p>(f) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or</p> <p>(g) biometric templates.</p> <p>(Schedule 5 (Dictionary) of the IP Act)</p>
<b>RTI</b>	Right to Information
<b>RTI Act</b>	<i>Right to Information Act 2009</i>

## Policy documents

Related policy documents:

- GOV-005 2024 P *Privacy and data breach policy*
- GOV-005 2024 PR2 *Data and privacy breach procedure*
- GOV-006 2024 P *Access to and amendment of information policy*
- GOV-006 2024 PR *Access to and amendment of information procedure*

## Related documents

- *Ombudsman Act 2001* (refer to s 92)
- *Inspector of Detention Services Act 2022* (refer to s 30)
- *Information security policy* (IS18:2018)
- *QGEA Information security incident reporting standard*
- *General Retention and Disposal Schedule*
- *ICT Incident Management Policy and Procedures*
- *Complaints Management System Policy*

- *Prevention and management of fraud and corruption policy and procedure*
- *Access to information policy*
- *Access to information procedure*
- *Data and privacy breach procedure*

## Policy owner

General Counsel

## Approval

Action	Officer	Date
<b>Author</b>	Alex Andrews Advisor, Right to Information and Privacy	19 / 2 / 2025
<b>Endorsed</b>	Christine Jones General Counsel	25 / 2 / 2025
<b>Approved and authorised for external publication</b>	Anthony Reilly, Queensland Ombudsman and Inspector of Detention Services	25 / 2 / 2025

## Document control

Version	Amendment history	Date
1	Draft	13 / 02 / 2025
2	Final	25 / 02 / 2025
3	Amendments to implement legislative changes made by the <i>Information Privacy and Other Legislation Amendment Act 2023</i> , coming into force on 1 July 2025.	1 / 7 / 2025