

Policy number	GOV-005 2024 P
eDocs	239705
Type	Policy
Status	Final
Classification	Public

# Data and privacy breach policy

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

## Audience

All staff, including contractors and volunteers.

## Purpose

This policy outlines obligations in relation to the collection, management, use and disclosure of personal information held by the Office.

This policy also outlines how the Office will respond to a data breach (or suspected data breach) and/or a privacy breach. The policy sets out the principles that will be applied in containing, assessing and managing a data or privacy breach incident.

## Policy statement

The Office is committed to managing all information held, in whatever form, in accordance with the *Public Records Act 2023*, *Right to Information Act 2009*, *Information Privacy Act 2009* and other relevant subordinate legislation, policies and standards.

The Office is also committed to the responsible handling of personal information that it collects, holds, uses and discloses in the discharge of its functions under the *Ombudsman Act 2001*, the *Inspector of Detention Services Act 2022* and the *Public Interest Disclosure Act 2010*.

The Office will respond to any data or privacy breach to prevent further breaches and mitigate the impact on affected individuals. In turn, this will reduce the costs associated with dealing with breaches and reduce reputational damage that can result.

## Principles

The following principles guide the interpretation and application of this policy, the *Privacy Plan* and the *Data and privacy breach procedure*:

Principle	What this means for the Office
<b>Compliant</b>	<ul style="list-style-type: none"> <li>The Office takes reasonable steps to protect the personal information it holds in accordance with the <i>Information Privacy Act 2009</i> (IP Act)</li> <li>The Office complies with the Queensland Privacy Principles (QPPs) when dealing with personal information.</li> </ul>

<b>Proactive</b>	<ul style="list-style-type: none"> <li>• This Office takes a 'Privacy by Design' approach.</li> <li>• Personal information is only collected where it is necessary for the Office's functions.</li> <li>• Privacy Impact Assessments are undertaken for new projects to identify potential privacy impacts.</li> <li>• Multiple systems and processes protect personal information held by the Office from misuse, interference, loss, unauthorised access, modification or disclosure.</li> <li>• All staff are informed of their responsibility to protect personal information and actions to take if a data or privacy breach is detected.</li> </ul>
<b>Prompt</b>	<ul style="list-style-type: none"> <li>• Immediate steps will be taken to contain and mitigate any data or privacy breach that occurs.</li> </ul>
<b>Responsive</b>	<ul style="list-style-type: none"> <li>• Each breach will be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.</li> </ul>

## Requirements

### *Privacy plan*

The IP Act regulates how public sector agencies and statutory bodies, such as the Office, must manage personal information. It creates an obligation to comply with the 13 Queensland Privacy Principles (QPPs) which are contained in Schedule 3 to the IP Act.

'Personal information' is defined broadly in the IP Act and it is important to note that information does not need to be particularly sensitive or confidential to be 'personal information'. 'Personal information' is not limited to directly identifying information such as a person's name.

The QPP privacy policy sets out how personal information held by the Office is collected, managed, used and disclosed.

### *'Privacy by Design'*

QO will only collect personal information where the information is reasonably necessary for, or directly related to, our functions or activities.

When we collect 'sensitive information' about an individual, we only do so in accordance with the IP Act (including QPP 3). Usually this means obtaining consent, or that the collection of information is required or authorised by law (for example, under the Ombudsman Act).

For new projects and processes, a Privacy Impact Assessment (PIA) is used to assess the privacy impacts and, where necessary, identify ways in which the obligations set out in the IP Act can be met.

A PIA will usually be necessary for projects and proposed processes where personal information is collected, stored, used, disclosed or transferred overseas.

The project manager for every new project (including new policy and procedure development) must consult the Advisor, RTI/IP who will assess whether a PIA is required. If a PIA is required, the Advisor, RTI/IP will conduct the PIA and provide recommendations to the project owner.

## ***Managing data and privacy breaches***

A data breach occurs when information is subject to unauthorised access, unauthorised disclosure, or loss (in circumstances where unauthorised access or disclosure is likely to occur from the loss).

If the information that is accessed, disclosed or lost is an individual's personal information a data breach is also a privacy breach.

A privacy breach occurs when personal information is accessed, used or disclosed without authorisation, or is lost, or otherwise dealt with in a way that would not comply with the IP Act. This may result from a data breach or where an agency does not comply with the QPPs (e.g. if an agency does not give sufficient notice to a person about collecting their information or does not collect the information for a lawful purpose related to the Office's functions).

In the event of a data or privacy breach, QO will follow the process set out in the *Data and privacy breach procedure*.

## ***Privacy complaints***

Individuals may complain to QO about a breach of the QPPs. The process for making a complaint is set out in the *Privacy complaint procedure*.

## ***Records management***

The *Public Records Act 2023* requires the Office to make and keep complete and reliable records of its activities in accordance with the *Records governance policy* (Queensland State Archives).

Records should be stored in accordance with the *Records management policy*.

The Advisor, RTI/IP will maintain a register for all data/privacy breaches.

All members of an ERT established to respond to a breach must ensure that all records are provided to the Advisor, RTI/IP for retention.

## ***Human rights considerations***

As required by the *Human Rights Act 2019*, QO will consider human rights, including section 25 concerning the right to privacy and reputation, in implementing:

- this policy
- the *Data and privacy breach response procedure*
- the *Privacy complaint procedure*.

## **Responsibilities**

<b>Officer</b>	<b>Authority</b>
<b>General Counsel</b>	<ul style="list-style-type: none"> <li>• Oversee and monitor policy outcomes</li> <li>• Identify legal obligations and provide advice</li> </ul>
<b>Advisor, Right to Information and Privacy</b>	<ul style="list-style-type: none"> <li>• Support the principles of 'Privacy by Design'</li> <li>• Undertake Privacy Impact Assessments</li> <li>• Records management</li> </ul>

## Definitions

Term / Acronym	Definition
<b>Advisor, RTI/IP</b>	Advisor, Right to Information and Privacy
<b>Data breach</b>	A data breach occurs when Office information is subject to unauthorised access, unauthorised disclosure, or loss (in circumstances where unauthorised access or disclosure is likely to occur from the loss).
<b>Privacy breach</b>	A privacy breach occurs when personal information is accessed, used or disclosed without authorisation, or is lost, or otherwise dealt with in a way that would not comply with the <i>Information Privacy Act 2009</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>OIC</b>	Office of the Information Commissioner
<b>Ombudsman</b>	Queensland Ombudsman and Inspector of Detention Services
<b>Personal information</b>	Personal information is defined in the IP Act as: Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion— (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
<b>PIA</b>	Privacy Impact Assessment
<b>QPPs</b>	Queensland Privacy Principles
<b>RTI</b>	Right to Information
<b>Sensitive information</b>	Under the IP Act, sensitive information for an individual means information or an opinion, that is also personal information, about the individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information about the individual, genetic information about the individual that is not otherwise health information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification or biometric templates.

## Legislation

- *Information Privacy Act 2009*
- *Human Rights Act 2019* (refer section 25 Privacy and reputation)
- *Public Records Act 2023*

## Policy documents

Related policy documents:

- GOV-005 2024 PR1 *QPP privacy policy*
- GOV-005 2024 PR2 *Data and privacy breach response procedure*
- GOV-005 2024 PR3 *Privacy Complaint Procedure*

## Related documents

- ICT Incident Management Policy and Procedures
- Complaints Management System Policy

## 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 / 2 / 2025
2	Final	25 / 2 / 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