

## Purpose

This policy sets out how the Office of the Health Ombudsman (OHO) will fulfill its obligations in relation to the access to, and amendment of information under the *Right to Information Act 2009* (RTI Act).

## Application

This policy applies to all OHO staff (permanent, temporary, agency), and contractors.

## Legislative provisions

- *Right to Information Act 2009*
- *Right to Information Regulation 2025*
- *Information Privacy Act 2009*
- *Electronic Transactions (Queensland) Act 2001*
- *Public Records Act 2023*
- *Health Ombudsman Act 2013*
- *Human Rights Act 2019*
- *Victims' Commissioner and Sexual Violence Review Board Act 2024 (Qld)*

## Related resources

- OHO Right to Information procedure
- OHO Administrative access policy
- OHO Administrative access procedure
- OHO Queensland Privacy Principles Policy
- OHO Recordkeeping Policy
- Office of the Victims' Commissioner Charter of Victims' Rights

## Policy statement

The Queensland Government has made a commitment to provide access to information held by the Government, unless on balance it is contrary to the public interest to provide that information.

The right to Information process aims to make more information available, provide equal access to information across all sectors of the community, and provide appropriate protection of an individuals' privacy.

The OHO recognises an individual's right to apply for access to, or amendment of information in the OHO's possession or control and is committed to considering requests for information with a pro-disclosure bias, unless the information is exempt or, on balance, contrary to the public interest to release.

## Accessing personal information

The OHO considers formal applications under the RTI Act should only be necessary as a '*last resort*' and wherever possible, information should be released administratively.

While the OHO's Administrative Access policy details the principles and circumstances in which administrative access may apply, information that may be released administratively could include:

- any documents the applicant may have given the OHO;
- any documents the OHO has previously given to the applicant (e.g. notices);
- OHO policies and procedures captured under the OHO's publication scheme; and
- other non-sensitive information.

An individual may request to access their personal information held by the OHO by making a request under the RTI Act<sup>1</sup>. The RTI Act gives an individual the right to access and amend such information, unless there is a good reason not to. As an example, an individual may not get access to other people's personal information, or information about or which forms part of an active investigation.

Any RTI application must be made to the OHO in writing, and must include:

- the applicant's name
- the applicant's address (includes an email address)
- evidence of the applicant's identity, most commonly a complete certified copy by a Qualified Witness of the applicant's identification document/s (e.g. driver's licence, passport, birth certificate) and, if the applicant is acting on behalf of another individual, evidence of their authority to access that individual's information, such as:
  - the will or court order appointing the applicant to act on behalf of the individual
  - the client agreement authorising a legal practitioner to act for the individual
  - where the individual is a child, evidence the applicant is the child's parent.

Further, certified copies of identity documents submitted by applicants who are also a qualified witness for the same application will not be accepted.

Exceptions to providing certified copies apply, for:

- applicants who are prisoners where they may provide a copy of their prisoner identity card certified by a corrective services officer
- applicants using the Queensland Digital Licence app may produce a PDF version of the digital authority contained in the app, this being a driver licence, photo identification card or personal watercraft licence or recreational marine drivers licence.

Certified copies of documents can be provided electronically to assist applicants simplify the application process<sup>2</sup>.

<sup>1</sup> Section 24, *Right to Information Act 2009*

<sup>2</sup> Section 16, *Electronic Transactions (Queensland) Act 2001*



The applicant must also provide sufficient information about the documents or information they are seeking, which could include details such as whether the information is the applicant's personal information or someone else, names of persons featured in the information sought, relevant case file references, information/document types, relevant dates, or other details reasonably known to the applicant.

In some circumstances, an application fee may apply when making a right to information request, and the application will not be processed until the fee is paid.

If the OHO denies an individual access to or amendment of information, written reasons will be provided to the applicant as required under the RTI Act.

Information about how to apply for access under the RTI Act and access an application form can be found on the OHO's [Request Information](#) webpage.

## Amending personal information

If an individual believes personal information held by the OHO is inaccurate, incomplete, out of date, or misleading they may request to amend this information under the RTI Act<sup>3</sup>.

To apply for amendment, the application must be made to the OHO in writing and be accompanied by a certified copy of the applicant's identification or authority document/s (as outlined above), as well as include:

- sufficient information concerning the document to enable the OHO to identify the document
- the applicant's address (includes an email address)
- detail the information of concern and how it is claimed to be inaccurate, incomplete, out of date, or misleading
- detail the amendments necessary to make the information accurate or not misleading, or the other information necessary to bring the information up to date.

## Review Rights

Where an applicant does not agree with the OHO's decision, they have the right to request a review, either to the OHO or to the Office of the Information Commissioner within particular timeframes.

### Internal – OHO review

A request for an internal review may be made to the OHO under the RTI Act<sup>4</sup>. The request must be made in writing, within twenty (20) business days from the date of the decision notice.

The Health Ombudsman as the Principal Officer of the OHO may delegate the internal review of an application to an officer who is to be no less senior than the original decision maker. The reviewing officer is required to consider the original decision with fresh eyes and in accordance with the provisions of the RTI Act.

There are no additional charges to the applicant for an internal review to be undertaken.

---

<sup>3</sup> Chapter 3A, *Right to Information Act 2009*

<sup>4</sup> Part 8, *Right to Information Act 2009*



## External – Office of the Information Commissioner

Alternatively, an applicant may also request an external review through the Office of the Information Commissioner (OIC)<sup>5</sup>. Again, such a request must be made in writing within 20 business days of the date of the decision notice.

## Human rights compatibility

- The OHO is committed to respecting, protecting and promoting human rights.
- Under the *Human Rights Act 2019* (HR Act) the OHO has an obligation to act and make decisions in a way that is compatible with human rights and, when making a decision, to give proper consideration to human rights.
- When considering an application, the decision maker must also identify and give consideration to any potential human rights limitation resulting from any related actions or decisions, ensuring the OHO remains compliant with its obligations under the HR Act.

## Roles and responsibilities

### Health Ombudsman

Under the RTI Act, the Health Ombudsman is considered to be the *Principal Officer* and is responsible for dealing with access and amendment applications.

The Health Ombudsman may delegate the responsibility for dealing with these applications and internal reviews under the RTI Act to certain employees, such as to the Senior Release of Information Officer.

### Senior Release of Information Officer

The Senior Release of Information Officer (SROI) typically has the day-to-day responsibility dealing with access and amendment applications made under the RTI Act, including:

- acting as the OHO's first point of contact for RTI applicants
- conducting an initial assessment of an RTI application to ensure the application is compliant with the requirements of the RTI Act, as well as whether the information requested is not already publicly available to the applicant or could be administratively released to the applicant
- liaising with OHO divisions regarding access documents, either administratively or under the RTI Act
- making decisions regarding the release of documents within legislated timeframes under the RTI Act
- providing a formal written notice of decision regarding the release of information to the applicant.

The SROI is an independent decision maker under the RTI Act.

---

<sup>5</sup> Part 9, *Right to Information Act 2009*

It is an offence under the RTI Act to give oral or written direction to the decision maker that the decision maker does not think should be made.

## Directors and Managers

Directors are responsible for ensuring:

- employees under their supervision are aware of, and act in accordance with all relevant record keeping and information privacy legislation (including OHO policies, procedures, guidance materials), as well as complete any relevant record keeping and information privacy training to ensure records are created and managed appropriately
- any assistance necessary is provided to the Principal Officer (or delegate) when searching for records within the OHO's responsibility
- a written statement is provided to the requesting party should information not be able to be located. This statement must include an acknowledgment that all reasonable steps have been taken to locate the information.

## All Staff

All permanent and temporary OHO staff, agency staff, and contractors must ensure that they:

- maintain all records within their workspace in accordance with all OHO record keeping policies, procedures, guidelines and directives
- provide assistance to the Principal Officer (or delegate) to ensure that any request for the provision of information is handled appropriately to ensure that legislated timeframes are met
- act in accordance with this policy, and all relevant policies, procedures, and legislation
- ensure they remain current and up to date with all relevant learning modules, and current relevant OHO policies and procedures.

Definitions	
Manager	For the purpose of this policy a manager includes anyone supervising an employee at the Office of the Health Ombudsman.
Personal Information	<p>As defined in section 12 of the <i>Information Privacy Act 2009</i>, personal information means information or an opinion about an identified individual or an individual who is <i>reasonably</i> 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>Personal information is held by a relevant entity, or the entity holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity.</p>
Principal Officer	Means the Health Ombudsman: See Schedule 5 of the <i>Right to Information Act 2009</i> and <i>Information Privacy Act 2009</i> (Definition of <i>Principal Officer</i> , subsection (f)) and section 257 of the <i>Health Ombudsman Act 2013</i> .



Qualified Witness	Means a lawyer or notary public, commissioner for declarations, a justice of the peace, or a pharmacist as defined at regulation 4 of the <i>Right to Information Regulation 2009</i> (Qld).
-------------------	--

Version control	
Version no.	Changes made
1.0	New document drafted

Approval	
Effective date	5 August 2025
Last reviewed	5 August 2025
Next review	5 August 2028
Contact	Senior Release of Information Officer
Custodian	Executive Director, Legal Services
Approved by	Health Ombudsman
Approval date	8 August 2025
Signature	
Security classification <sup>6</sup>	Official

<sup>6</sup> NB. This footnote is intended to provide guidance when deciding the security classification of information.

Official – routine information without special sensitivity or handling requirements and a low business impact per document if compromised or lost. For example, information that may be shared across government agencies.

Sensitive – information that requires additional handling care due to its sensitivity or moderate business impact if compromised or lost. For example, information containing legal professional privilege.

Protected – information that requires the most careful safeguards due to its sensitivity or major business impact if compromised or lost. For example, cabinet documents.