Queensland Human Rights Commission

Data breach policy

Issued 1 July 2025

Queensland Human Rights Commission

Contents

1. Audience

This policy applies to all Queensland Human Rights Commission (QHRC or Commission) employees. For the purpose of this document, employee means:

- any employee, whether permanent, temporary, full time, part time or casual and includes the Commissioner, and
- any volunteer, student, contractor, consultant, agency temp, secondee or anyone who works in any other capacity for the Commission.

2. Purpose

The purpose of this policy is to provide the steps for QHRC staff to take in the event of a data breach. These steps aim to facilitate a timely and effective response to a data breach, and avoid or mitigate potential harms to individuals, QHRC and other entities.

The Commission is subject to the requirements of the *Information Privacy Act 2009* (Qld) (IP Act). Chapter 3A of the IP Act provides a scheme for the management and mandatory notification of eligible data breaches (MNDB scheme).

In addition, under section 220 of the *Anti-Discrimination Act 1991* (Qld), QHRC staff must not communicate or disclose information about a person's affairs unless it is required for the performance of a function in connection with that Act or is required or permitted by another Act.

3. Scope

The scope of this policy covers preparation, identification, management and prevention of data breaches.

A *data breach* is the unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.

A data breach involving personal information and likely to result in serious harm to an individual to whom the personal information relates is referred to as an *eligible data breach*.

Personal information is 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.

The MNDB scheme requires QHRC to follow specific steps when dealing with a suspected data breach. Where QHRC knows or reasonably suspects that a data breach is an eligible data breach, QHRC must do the following:

(a) **Containment**. Immediately take all reasonable steps to contain the data breach and mitigate the harm caused by the data breach.

(b) **Assessment**. If there is uncertainty as to whether the data breach is an eligible data breach, assess whether there are reasonable grounds to believe the data breach is an eligible data breach within 30 days.
(c) **Notification**. If the Commission knows or reasonably believes that the data breach is an eligible data breach, the Commission must, as soon as practicable, notify the Information Commissioner and particular individuals.

4. Policy statement

Data breaches can have serious and harmful consequences for:

- affected individuals, such as financial fraud, identify theft, damage to reputation, violence, or psychological harms, and
- the QHRC and other entities, such as negative impacts on reputation, finances, interests or operations, and loss of confidence and trust.

The right to privacy imposes obligations on public entities to do what is necessary and reasonable to protect personal information and safeguard against its misuse. A data breach involving personal information impacts the person's right to privacy. Depending on the type of personal information and circumstances surrounding the breach, there could be consequences and flow-on effects to other rights such as liberty and security, a fair hearing or right to protection from torture and cruel, inhuman or degrading treatment. In the event of a breach, emphasis is placed on the importance of measures of containment and mitigating harm to the person(s) involved.

The MNDB scheme addresses these issues and is consistent with human rights. By preparing this policy in compliance with the MNDB scheme and having given proper consideration to the human rights outlined above, QHRC considers this policy is compatible with human rights. When making decisions or acting under this policy, decision-makers must comply with those human rights obligations.

5. Roles and responsibilities

All staff are responsible for handling personal information in accordance with QHRC's privacy obligations.

Managers and **supervisors** of each team are responsible for supporting a culture of privacy protection.

Where there is an actual or suspected data breach:

(a) **All staff** are responsible for notifying their supervisor and the Privacy Officer of any actual or suspected data breaches as soon as possible.
(b) **Managers** and **supervisors** of each team are responsible for supporting staff to contain breaches to mitigate harm, report the breach to the Privacy Officer and, where appropriate, notify the relevant Director.
(c) **Privacy Officer** is responsible for receiving, assessing and responding to breaches in accordance with this policy and providing sufficient training opportunities and awareness-raising materials to enable staff to meet their obligations under this policy.

6. Policy

The key concepts of this policy relate to preparation activities, identification of a suspected data breach, management of data breaches and prevention controls.

An incident can arise in almost any part of a business, whether it is internal, client-facing or vendor-related. They can result from human error, system failures, inadequate policies and training, misunderstanding of requirements or deliberate acts. They can be identified through information provided by a complainant, the review of processes or systems, or self-reporting of an error or loss.

QHRC holds information both in its physical possession, or under QHRC's control (such as where it has been provided to others such as a law firm for legal advice). Where an incident relates to QHRC's information (a data related incident), a conservative approach is taken, and it is treated as a potential or suspected data breach.

6.1. Key preparation activities and controls

QHRC identifies and prevents data related incidents and data breaches through key controls such as:

(a) completion of staff training on information privacy and security as part of induction and on an ongoing basis
(b) information privacy and security awareness updates to all staff
(c) processes in place guiding the handling of personal information from pre-collection, once collected, while it is held and once no longer needed
(d) appropriate management of electronic information in secure locations
(e) system access policies and multi-factor authentication in place
(f) use of privacy impact assessments for business projects or decisions that involve new or changed personal information handling practices
(g) established processes for receiving and responding to privacy enquiries and complaints, including a designated Privacy Officer
(h) QHRC executive management committee reporting and oversight.

Where third party service providers hold information for or on behalf of QHRC, QHRC ensures the provider:

(a) has sufficient protections in place against data loss, unauthorised access, use, modification or disclosure,
(b) is required to report any data breaches affecting QHRC's data to QHRC.

6.2. Identifying a suspected data breach

Upon identification of a suspected data breach staff are expected to promptly contact and consult with their supervisor and/or the Privacy Officer. An incident is any event, error or failure that may lead to loss or harm to QHRC, its clients, or staff. Any data related incident is treated as a suspected data breach.

The below table provides examples of suspected data breaches:

Potential causes	Examples
(a) Unauthorised access	(i) an employee intentionally views or uses information for a purpose unrelated to their work (ii) QHRC is subject to a cyber-attack.
(b) Unauthorised disclosure	(i) unintended publication of personal information (ii) email sent to the wrong recipient (iii) file share that is accessed by unauthorised persons.
(c) Loss of information, where unauthorised access or unauthorised disclosure is likely to occur	(i) printing containing sensitive information is left in a communal space in the office (ii) a hard copy file is left on the bus (iii) a staff member's laptop is stolen which has information stored on the local hard drive.

6.3. Data breach management

In the event a data breach is identified staff must follow the steps below.

6.3.1. Containment

Step 1. Take all reasonable steps to contain the data breach and mitigate the harm.

On identification of a suspected data breach, staff may be able to undertake some initial containment action. This is important if unauthorised access or disclosure is still occurring to ensure harm is appropriately mitigated.

Any containment action undertaken must not destroy information that is needed to investigate the breach and prevent a recurrence. The extent and kind of containment action necessary will depend on the type of breach. These ongoing containment activities may continue while the breach is being managed.

The table below provides examples of incidents and suggested containment action.

Example breach	Suggested containment action
(a) Email containing personal information sent to incorrect recipient.	Ask the recipient to delete the email and request that the recipient confirms deletion of the information in writing.
(b) Internal system releasing personal information incorrectly.	Contact QHRC ICT immediately to suspend the system and stop all data release.
(c) Unauthorised access to a work device.	Contact QHRC ICT immediately to change passwords and any other access requirements to the device.
(d) Unauthorised access to a work database containing personal information.	Contact QHRC ICT immediately and ask them to review all users with access to the database and restrict access as necessary. Password changes will also need to be considered.
(e) Cyberattack, phishing attack or evidence of a malicious actor targeting QHRC.	Contact QHRC ICT immediately for action.

6.3.2. Internal notification

Step 2. Provide sufficient information to the Privacy Officer for the breach to be properly assessed.

The Privacy Officer should be provided with enough information for the incident to be properly assessed, particularly any containment action taken. This includes:

(a) notification date
(b) date the breach was identified
(c) how information was lost or accessed
(d) how the breach was identified
(e) nature of the information lost or accessed
(f) number of individuals impacted (if known)
(g) initial steps taken to contain loss or access and mitigate harm caused by the breach (if any)
(h) any other information, concerns or risks, e.g. likelihood of access and by whom
(i) name of the QHRC staff member making the notification
(j) name of the QHRC staff member's supervisor.

It is important that all data related incidents are acted upon as soon as identified. Depending on the nature of the data breach, the Privacy Officer may consult key management personnel within QHRC including:

(a) senior management responsible for the area in which the breach occurred
(b) the Commissioner
(c) senior personnel responsible for information security, governance, communications, legal services and human resources.

6.3.3. Privacy Officer assessment

Step 3. The Privacy Officer will coordinate the assessment, further containment and classification of the data breach.

The Privacy Officer will assess containment action that has been undertaken, and coordinate any further steps necessary to:

(a) contain the breach
(b) minimise any ongoing damage from the breach, and
(c) prevent any further similar breaches.

Once the breach is contained, the Privacy Officer will assess whether the breach is a data breach or an eligible data breach. This assessment must be recorded and relevant QHRC staff notified of the outcome.

The assessment of whether a data breach is an eligible data breach is twofold. Firstly, does the data breach involve personal information? If no, the data breach is not an eligible data breach. The second consideration is whether the data breach is likely to result in serious harm to the individual. If yes, the data breach is an eligible data breach. Appendix A sets out the process steps and further considerations in making an assessment as to whether a data breach is an eligible data breach.

The assessment of whether a data breach is an eligible data breach must be completed within 30 days of the breach event. If an extension is required to complete the assessment, QHRC must contact the Information Commissioner before the 30 day assessment period ends and confirm:

(a) the assessment has commenced
(b) QHRC has extended the timeframe for completing the assessment, and
(c) the new date for the assessment to be completed.

Where the Privacy Officer assesses a breach to be an eligible data breach, that advice must be reviewed and confirmed by the Director, Corporate Services. For data breaches that involve personal information, but are not eligible data breaches, QHRC's privacy breach policy procedure applies.

6.3.4. External notification

Step 4. The Privacy Officer will take all relevant disclosure actions

Under the IP Act, the requirement to notify only applies to eligible data breaches. However, in accordance with the right to privacy, QHRC will consider notifying affected individuals in all data breaches involving personal information.

The Privacy Officer is responsible for liaising with any external stakeholders who may be affected by the data breach, notifying the relevant parties and managing their responses.

The Privacy Officer will also consider whether:

(a) The Commission has any other mandatory notification obligations under other legislation, such as the *Privacy Act 1988* (Cth); and
(b) any other entities which must be notified of the breach depending on the circumstances, for example:
    (i) the Attorney-General and Minister for Justice
    (ii) the Crime and Corruption Commission Queensland if the breach involves corrupt conduct
    (iii) Queensland Government Information Security Virtual Response Team for cyber and information security incidents
    (iv) Queensland Government Insurance Fund for a cyber security incident that results in a loss
    (v) Queensland Police Service if the breach appears to involve theft or other criminal activity; and
    (vi) the State Archivist if the breach involves the loss or unauthorised destruction of a public record.

For eligible data breaches, the Privacy Officer will notify the following:

(a) the Information Commissioner
    (i) The Privacy Officer will prepare and send a statement to the Information Commissioner which contains the information prescribed under section 51 of the IP Act.
(b) affected individuals, QHRC may notify (in order of priority):
    (i) each individual whose personal information was accessed, disclosed or lost
    (ii) each *affected* individual, that is, the individual to whom the information relates and who is likely to suffer serious harm because of the breach, or

(iii) publish the required information on QHRC's website (and the Information Commissioner's website) for a period of at least 12 months.

The requirement to notify individuals who have been affected by the breach will depend on the nature and extent of the breach. Depending on what is reasonably practicable in the circumstances.

QHRC is not required to comply with these notification requirements if:

(a) complying with the obligation would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal
(b) the eligible data breach involves another agency and that agency is undertaking the notification obligations
(c) QHRC has taken specified remedial action so that the information was not accessed or disclosed or serious harm is no longer likely to occur
(d) compliance would be inconsistent with a law that regulates the use or disclosure of the information
(e) compliance would create a serious risk of harm to an individual's health or safety, or
(f) compliance is likely to compromise or worsen QHRC's cybersecurity or lead to further data breaches.

6.4. Record keeping

The Privacy Officer is responsible for keeping records of data breach responses and management. QHRC keeps an internal register of eligible data breaches.

Following notification, the Privacy Officer will include the following information in the register:

(a) a description of the eligible data breach
(b) the date notification was given to the Information Commissioner
(c) the date individuals were directly notified about the eligible data breach, including who was notified, when and how
(d) if relevant, any exemption relied on to justify a decision to not notify
(e) the steps taken to contain the eligible data breach and mitigate its harm, and
(f) the actions taken to prevent future data breaches of a similar kind occurring.

6.5. Post incident review and prevention

Following any data breach an assessment will be carried out to identify the root cause of the incident, any control weakness and what steps can be taken to prevent reoccurrence. Depending on the seriousness of the incident, such steps may include:

(a) reviewing access controls to databases
(b) reviewing or updating policies and procedures in relation to the collection, storage and management of information
(c) refresher privacy training for the relevant staff members
(d) reviewing service provider training and contractual obligations; and
(e) identifying any new controls (preventative, detective or corrective) which could be implemented to prevent a similar breach in future.

The review may be carried out by the Privacy Officer in conjunction with the business area involved or performed as part of a broader controls assessment or internal audit review.

7. Definitions

Term	Meaning
ARC	QHRC's Audit and Risk Committee
Commission	Queensland Human Rights Commission
Commissioner	Queensland Human Rights Commissioner
Data breach	The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
Eligible data breach	A data breach involving personal information and likely to result in serious harm to an individual to whom the personal information relates.
Incident	Any event, error or failure that may lead to loss or harm to the Commission, its clients, or staff.
Information Commissioner	Queensland's Information Commissioner
IP Act	*Information Privacy Act 2009* (Qld)
MNDB	Mandatory notification data breach scheme under the IP Act
Personal information	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.
Privacy breach	A privacy breach occurs when QHRC does not comply with the QPPs as outlined in this document.
Privacy Officer	The Privacy Officer is a designated role at QHRC and can be contacted at privacy@qhrc.qld.gov.au.
QHRC	Queensland Human Rights Commission

Term	Meaning
Sensitive information	Information or an opinion about an individual's: (a) racial or ethnic origin (b) political opinions (c) membership of a political association (d) religious beliefs or affiliations (e) philosophical beliefs (f) membership of a professional trade association (g) membership of a trade union (h) sexual orientation or practices (i) criminal record (j) health information (k) genetic information that is not otherwise health information (l) biometric information that is to be used for the purpose of automated biometric verification or biometric identification or (m) biometric templates
Serious harm	Serious harm to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or (b) serious harm to the individual's reputation because of the access or disclosure.

8. Reporting requirements

Eligible data breaches will be notified to the Information Commissioner in accordance with this policy. The Commission also maintains an internal register of any eligible data breaches and has published this policy on the Commission's website.

9. Related documents

1. *Anti-Discrimination Act 1991 (Qld)*
2. *Information Privacy Act 2009* (Qld)
3. *Human Rights Act 2019* (Qld)
4. QHRC privacy policy

10. Document control

This policy will be reviewed at least on an annual basis.

Version	Date	Author	Approver	Details
1.0	1 July 2025	Director, Corporate Services	Commissioner	New policy.

Appendix A: Assessing whether a data breach is an eligible data breach

Step 1: Unauthorised access, disclosure or loss of personal information

This step involves making an assessment as to whether:

(a) there has been unauthorised access to or disclosure of personal information; or
(b) personal information is lost and unauthorised access or disclosure is likely.

If personal information has been lost, accessed or disclosed without authorisation, QHRC will continue to step 2.

If the data breach does not involve personal information, an eligible data breach has not occurred. However consideration should be given to any external notifications required and any post incident review and prevention measures.

Step 2: Serious harm assessment

The serious harm assessment step is broken into two parts:

(a) QHRC will assess whether the data breach could cause serious harm to the individual that it relates to. In making this assessment the following factors are relevant (this list is not exhaustive):
    (i) the kind of personal information accessed, disclosed or lost
    (ii) the sensitivity of the personal information
    (iii) whether the personal information is protected by security measures and the likelihood that any of those security measures could be overcome
    (iv) the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information
    (v) the nature of the harm likely to result from the data breach, and
    (vi) any other relevant matter.
(b) The second part of the serious harm assessment step is where QHRC assesses whether the serious harm is likely to occur. This is assessed on a case by case basis. Whether serious harm is likely to occur requires that the risk of serious harm to an individual must be more probable than not to occur. If the breach could cause serious harm that is likely to occur, then it is an eligible data breach. QHRC will consider notification and other measures in accordance with the QHRC data breach policy. If the breach would not cause serious harm, or serious harm is unlikely to occur, then it is not an eligible data breach. QHRC would then apply the QHRC privacy policy.

The below diagram provides a high level overview of the process for assessing whether a data breach is an eligible data breach.

Figure 1: Assessing whether a data breach is an eligible data breach