Mandatory Notification of Data Breaches Policy and Procedure

Scope

Applies to all QLeave employees (full-time, part-time, temporary, and casual).

Purpose

The purpose of this policy and procedure is to provide guidance on the mandatory notification of data breaches, ensuring compliance with relevant legislation and protecting personal information.

Policy Statement

QLeave is committed to protecting personal information and ensuring transparency in the event of a data breach. The Mandatory Notification of Data Breach (MNDB) Scheme under the *Information Privacy Act 2009* (Qld) (**IP Act**) only applies to 'eligible data breaches' involving 'personal information'.

This policy outlines the steps to be taken when a data breach occurs, including assessment, notification, and mitigation measures.

Responsibilities

Employees

- Immediately report any suspected data breaches to their direct supervisor.
- Assist in the assessment and containment of the data breaches.
- Follow all procedures outlined in this policy for managing data breaches.

Direct supervisor of employee's business unit where the breach occurred

- Ensure that any reported data breaches are promptly contained, with the support of the Information Technology & Innovation Team (**ITI**).
- Notify the Manager Legal Services of any suspected data breaches and assist in the assessment process.

Manager Legal Services / Legal Services Team

- Carry out assessment of data breaches to determine if they are 'eligible data breaches'.
- Maintain an internal register of 'eligible data breaches'.
- Notify affected individuals or their authorised representative of the information required in s 53(2) of the IP Act (**the required information**) (where reasonably practicable).
- Notify all eligible data breaches to the Office of the Information Commissioner (OIC) (unless an exemption applies).
- Ensure publication of required information on QLeave's website (if required).

Version number: 1.0	**Version effective:** 01/07/2025	**Next scheduled review:** 30/06/2028
Document ID: PPO-0088	**Approved by:** General Manager	**Content owner:** Legal Services

ITI Team

- Liaise and assist the Legal Services team and direct supervisor of applicable business units in responding to a suspected data breach.
- Provide all necessary data, information and reports to the Legal Services team in relation to suspected data breaches, where applicable and as required.
- Take steps to contain data breaches, in consultation with the Legal Services team.
- Assess the types of data that have been compromised in data breaches.

Principles

QLeave:

- will act swiftly to contain and assess any data breach to minimise potential harm.
- is committed to notifying affected individuals and relevant authorities as soon as practicable following a data breach that has been assessed as an 'eligible data breach'.
- will assess the nature and scope of the data breach to determine the potential impact on individuals and on QLeave.
- will take all reasonable steps to mitigate the harm caused by a data breach, including implementing measures to prevent future breaches.
- will maintain detailed records of data breaches, including the nature of the breach, actions taken, and outcomes.
- will regularly review and update its data breach response procedures to enhance effectiveness and ensure compliance with legislative requirements.
- is dedicated to protecting individuals' privacy and ensuring that personal information is handled in accordance with the IP Act and QLeave's administered legislation.

Overview and Requirements

Responding to a suspected data breach

Each data breach is unique and requires a tailored response. Response actions will depend on factors such as the types of data compromised, the cause of the breach, and the potential harms that could arise for affected individuals. It is important to understand the risks posed and respond to each breach accordingly.

While the details of each breach will be different, the process for responding to a data breach is always the same. The steps are as follows:

1. **Initial identification and triage**: Identifying, communicating and triaging breach reports.
2. **Contain**: Immediate action for containing the breach to prevent any further compromise of personal information.
3. **Assess and mitigate**: Assessing or evaluating the information involved in the breach and the risks associated with the breach to determine next steps and implementing any additional actions identified to mitigate risks.
4. **Notify**: Notifying the OIC and those affected by the eligible data breach.

What is an eligible data breach?

A data breach will be an 'eligible data breach'[1] where the breach involves:

[1] IP Act s 47(1).

- Unauthorised access to, or unauthorised disclosure of personal information, which is likely to result in **serious harm**[2] to an individual to whom the information relates.
- Loss of personal information where unauthorised access to, or disclosure of information is likely to occur and if it was to occur would be likely to result in **serious harm** to an individual to whom the information relates.

Regard must be had to the below matters in considering whether serious harm would be likely to result:

- The kind of personal information accessed, disclosed or lost; and
- The sensitivity of the personal information; and
- Whether the personal information is protected by 1 or more security measures; and
- If the personal information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome; and
- The persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and
- The nature of the harm likely to result from the data breach; and
- Any other relevant matter.[3]

Unauthorised access

Unauthorised access to personal information occurs when personal information held by QLeave is accessed by someone who is not permitted to do so.

Unauthorised access can occur:

- Internally within QLeave – for example, an employee browses QLeave records relating to a family member or a registered worker/employer without a legitimate purpose.
- Between agencies – for example, a team at QLeave may be provided with access to systems and data at a second agency as part of a joint project. Unauthorised access may occur if a member of the team were to use that access beyond what is required for their role as part of that project.
- Externally outside QLeave – for example, personal information is compromised during a cyberattack and accessed by a person external to QLeave.

Unauthorised disclosure

Unauthorised disclosure occurs when an agency (intentionally or accidentally) discloses personal information in a way that is not permitted by the IP Act.

For example, an unauthorised disclosure may occur where:

- A system update results in the unintended publication of customer records containing personal information on QLeave's website.
- QLeave intends to provide de-identified information to a third party but accidently sends the data with personal identifiers included.
- QLeave provides personal information to the wrong recipient regardless of whether the information was viewed or accessed by the recipient.

---

[2] *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.

[3] IP Act s 47(2).

- A database hosted in a cloud environment or a web facing application containing personal information does not have appropriate access controls and personal information in the data set is visible and accessed by unauthorised individuals.

Unauthorised access and disclosure are not mutually exclusive and may occur because of the same breach or as part of a chain of events. For example, if a malicious external actor gains unauthorised access to QLeave's records during a cyberattack, and steals information from those records, this may amount to unauthorised access to, and unauthorised disclosure of, the personal information held within those records.

Loss of personal information

Loss refers to situations in which personal information is removed from the possession or control of QLeave. Loss may occur because of a deliberate or accidental act or omission of QLeave, or due to the deliberate action of a third party. For example, personal information might be lost when:

- QLeave sells or disposes of a physical asset (such as a laptop or filing cabinet) that still contains personal information.
- A QLeave employee accidentally leaves a device containing personal information on public transport.
- A device containing personal information is stolen from QLeave's premises or an employee's home.

The loss of personal information will only result in an eligible data breach where such loss is likely to result in unauthorised access or disclosure of this information. If the personal information is inaccessible due to security measures or because the information is retrieved before it is accessed or disclosed, then it is unlikely that an eligible data breach has occurred.

Examples of this may include where:

- A password protected laptop containing client files is left on a bus but is handed into the depot and QLeave can retrieve the laptop which has not been accessed.
- A USB or mobile phone containing personal information is lost but is both encrypted and password protected.
- A tablet device containing client records is stolen from an employee's home, but it is only accessible via multifactor authentication.

As the loss of personal information in the above examples did not result in unauthorised access or disclosure, no eligible data breach has occurred.

In some cases, a loss that results in serious harm to an individual may not necessarily amount to an 'eligible data breach'. For example, where customer records are unintentionally deleted from a records management system, resulting in the denial of a particular service to those customers. Although this would not be an eligible data breach and notification is not mandatory in this scenario, it is nonetheless recommended the Manager of Legal Services consider voluntarily informing individuals of the loss of their information where there is a risk of serious harm.

Individual to whom the information relates and 'affected individuals'

When it has been determined that an eligible data breach has occurred, if reasonably practicable the Manager Legal Services should notify an 'affected individual'. An 'affected individual' is defined under s 47 of the IP Act as an individual:

- To whom the information subject to unauthorised access, unauthorised disclosure or loss relates, and
- Who a reasonable person would conclude is likely to suffer serious harm because of the data breach.

The phrase 'to whom the information relates' is not defined and should be given its ordinary meaning (i.e. the person who is the subject of the information).

An individual will be an affected individual, regardless of whether the information was originally collected directly from the individual or from a third party, if the information involved in the breach is about them.

Impacts on individuals, agencies or others that are indirectly connected to the breached information (but are not an 'individual to whom the information relates') should be excluded from the assessment for the purposes of the MNDB Scheme. In general, an individual who is only indirectly connected to the information involved in a data breach, for example through a family relationship or community group, and who may suffer detriment following a data breach because of that connection, would not ordinarily be an 'individual to whom the information relates'.

For example, if a data breach discloses that an individual has a serious communicable disease, members of that individual's family may suffer serious harm (for example reputational damage or discrimination) because of the disclosure. However, a family member in this scenario would not be a person to whom the information relates as they are not the subject of the information disclosed.

Procedure

1. Step 1 - Initial identification and triage

To respond to a data breach, QLeave must first know that it has occurred. Acting quickly when a breach is discovered or suspected is essential to reducing the impact for both QLeave and affected individuals.

When in doubt, a conservative approach should be adopted, and the suspected breach should be escalated to the employee's direct supervisor. Escalated incident response processes can be easily stood down if a breach turns out to be less serious than initially thought, but time lost when a serious incident is not escalated cannot be regained.

1.1 Obligations

Any QLeave employee who suspects that an eligible data breach has occurred must immediately report the suspected breach to their direct supervisor, who will consider the suspected breach. Their direct supervisor must report this to the Manager Legal Services for assessment and potential notification to the OIC.

2. Step 2 - Contain

'Containing' a data breach means limiting its extent or duration or preventing it from intensifying. This could be done by stopping an unauthorised practice, recovering or limiting the dissemination of records disclosed without authorisation, shutting down a compromised system or a combination of these actions. Containment actions can be distinguished from mitigation actions, which involve managing or remediating harms arising because of the breach.

2.1 Obligations

The direct supervisor of the employee's business unit where the breach occurred (in conjunction with ITI, depending on the nature of the breach) must immediately take all reasonable steps to contain the data breach upon discovery or suspicion of a breach, and ensure that no further unauthorised access or disclosure of personal information occurs.

If the breach may affect another agency, the Manager Legal Services (based on information provided from the direct supervisor/ITI) will provide written notice to the other agency with a description of the breach and the kind of personal information involved (including a description of the data breach and the kind of personal information the subject of the data breach, without including any personal information in the description).[4]

2.2 Possible containment measures

What efforts are reasonable to contain a breach will depend on the circumstances and severity of the breach, including:

- The type of data breach.
- Who has access to the personal information.

[4] IP Act s 48(4)(b).

- The extent to which the breached personal information is still being shared, disclosed or lost without authorisation.
- The degree of harm that may result from continued exposure or dissemination of the records and the likelihood of such harm occurring, noting that agencies should mitigate even minor harms unless the cost, time and effort required to do so are excessively prohibitive.
- The availability and suitability of containment measures, considering their effectiveness, their impact on other individuals or QLeave's operations, their practicality, and other relevant factors such as whether they would result in loss of evidence.

Context	**Example containment actions** *Some common types of containment actions include, but are not limited to*:
A letter has been sent to the wrong recipient.	Direct supervisor of the employee's business unit responsible for the breach to contact the recipient and request the deletion of the personal information they have received. If the personal information was highly sensitive, this could be evidenced by a statutory declaration or non-disclosure agreement.
A document is sent via a postal service and is lost in transit.	Direct supervisor of the employee's business unit responsible for the breach to: • Confirm (if possible) whether the document was properly addressed. • Contact the postal service to inquire as to the location of the document and whether it was confirmed as delivered. • Work with the postal service (if possible) to recover the document or confirm its destruction.
An email has been sent to the wrong recipient.	Direct supervisor of the employee's business unit responsible for the breach to contact the recipient to: • request they delete the email from their inbox and all trash items; and • seek confirmation they have not forwarded or printed the document. If the email or attachment was encrypted, it may be possible to remotely revoke access. If QLeave controls the recipient email inbox (for example, if the email was incorrectly sent to an internal recipient) it may be possible to recall or delete the email from the recipient inbox.
A physical asset (for example laptop, USB or mobile phone) containing personal information has been lost or misplaced.	ITI to remotely wipe the device.
A system failure has resulted in a computer system exposing or distributing personal information in an unintended way.	ITI to: • If practicable, shut down the system pending investigation and resolution of the issue.

	• Roll back to a previous software version that was not subject to the same issue.
A cyber-attack has led to the compromise of a system containing personal information.	ITI to: • Isolate the system or compromised area of the system pending full investigation and response. • In extreme cases, a full system shutdown may be required
An employee has misused their valid credentials to access or disclose personal information outside the scope of their duties.	ITI to suspend the employee's system access pending full investigation.

2.3 Third party service providers

Data breaches involving third-party service providers present unique challenges for QLeave, even with appropriate contractual obligations in place. For example, the service provider might be responsible for handling, storing or processing QLeave's data, and the breach occurs within the service provider's system, or the service provider has access to QLeave's systems or data, and the breach happens through this access.

When dealing with a third-party breach, the following should occur:

- The direct supervisor of the employee's business unit where the breach occurred to engage with the Procurement team to review relevant contracts to understand the parties' obligations.
- ITI and the direct supervisor of the employee's business unit where the breach occurred to work with the third-party vendor to understand the nature and extent of the breach.
- ITI to ensure the third-party vendor notifies QLeave of any breaches involving QLeave's data and cooperates in the containment and assessment process.

3. Step 3 - Assess and mitigate

3.1 Obligations

The Manager of Legal Services must assess whether there are reasonable grounds to believe the data breach is an 'eligible data breach' within 30 days of forming the suspicion (however, this may be extended to a period reasonably required for the assessment to be completed).[5]

In line with the responsibilities outlined above, all reasonable steps to mitigate the harm cause by the data breach (both during and after the assessment) must be taken by the Manager of the business unit where the breach occurred and ITI (depending on the type of breach).

3.2 Assessment

The direct supervisor of the employee's business unit where the breach occurred and ITI (depending on the type of breach) must:

- Collect all relevant information regarding the suspected breach. This may involve contacting relevant stakeholders, identifying what information was or may have been compromised, and investigating logs or other evidence from compromised systems that may be relevant to the assessment of the suspected breach.
- Determine how the breach occurred, the type of information involved, and the extent of the breach.

The Manager Legal Services will then:

[5] IP Act s 49.

- Assess the potential harm to affected individuals, considering factors such as the sensitivity of the information, the likelihood of misuse, and the number of individuals affected.
- In consultation with ITI, consider whether the personal information was protected by security measures and the likelihood that these measures could be overcome.

3.3 Mitigation measures

In practice, mitigation strategies will vary depending on the type and nature of the breach, and the potential harm to individuals the breach may cause. Notification, which enables affected individuals to take action to protect themselves, is the most common and most discussed mitigation measure. However, in many cases, additional mitigation steps are appropriate.

When a data breach affects certain individuals particularly severely, it may be appropriate to provide tailored support to meet their needs, which could include counselling, enhanced security, relocation assistance, or financial compensation.

When a data breach has an impact on a wider group of individuals, it may be more appropriate to focus on more scalable support options, such as helplines for advice about the breach, referral to specialist identity theft and cybersecurity counselling services such as ID Support, IDCare, or credit monitoring.

Other examples of mitigation measures include:

- ITI may be able to implement additional security measures within QLeave's systems and processes to limit the potential for misuse of compromised information. For example, by resetting passwords or adding additional requirements for proof of identity verification.
- QLeave may take steps to limit the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites. Where information has been published, ITI may be able to contact internet search engines to ensure compromised personal information is not indexed.
- QLeave may engage with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes, or to streamline the re-issue of compromised identity documents. For example, the direct supervisor of the employee's business unit where the breach occurred may contact an identity issuer or financial institution to advise caution when relying on specific identity documents for particular cohorts.

4. Step 4 - Notify

Once the assessment has been completed above, the notification process commences.

Transparency around how QLeave handles people's information is central to good privacy practice. This extends to transparency when there is a breach and any personal information QLeave holds is compromised.

Notifying affected individuals when a breach occurs allows them to take actions to protect themselves from harm and regain control of their information. Timely notification can be key to minimising the risks of serious harm resulting from a data breach.

4.1 Obligations

There are four steps in the notification process:

1. **Notify the OIC**: Once the Manager Legal Services determines an eligible data breach has occurred, the Manager Legal Services must notify the OIC about the breach as soon as practicable after forming the belief that the data breach is an eligible data breach (unless an exemption applies).[6]

2. **Determine whether an exemption applies:** If one of the six exemptions set out in the MNDB Scheme under the IP Act applies in relation to an eligible data breach, QLeave may not be required to notify affected individuals.

[6] See exemption contained under ss 55 – 60 of the IP Act.

3. **Notify individuals**: Unless an exemption applies, the Manager Legal Services is required to notify affected individuals or their authorised representative as soon as reasonably practicable after forming a reasonable belief that a data breach is an eligible data breach, of the information required in s 53(2) of the IP Act (**the required information**). Where the Manager Legal Services is unable to notify directly or it is not reasonably practicable to do so, QLeave must publish the required information on QLeave's website for a period of at least 12 months.

4. **Further information to be provided to the OIC:** QLeave may be required to provide additional information to the OIC, if it has been unable to provide complete information in its initial notification, if it has made a public notification, or if it is relying on an exemption.

4.2 Notification to the OIC

If the Manager Legal Services decides the data breach is an 'eligible data breach', or there are reasonable grounds to believe the data breach is an eligible data breach, then the Manager Legal Services will immediately notify the OIC.

In some cases, it may be obvious that a breach will be an eligible breach even before the assessment is completed. If this is the case, the Manager Legal Services should consider notifying the OIC immediately rather than waiting until the assessment is finalised.

To the extent it is reasonably practicable, the statement to the OIC must include:

- QLeave's name and, if more than one agency was affected by the data breach, the name of each other agency.
- The Manager Legal Services' contact details.
- The date the data breach occurred.
- A description of the data breach, including the type of eligible data breach.
- Information about how the data breach occurred.
- If the data breach involved unauthorised access to or disclosure of personal information—the period during which the access or disclosure was available or made.
- The steps QLeave has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach.
- A description of the kind of personal information the subject of the data breach, without including any personal information in the description.
- QLeave's recommendations about the steps individuals should take in response to the data breach.
- Whether QLeave is reporting on behalf of other agencies affected by the same data breach and, if so, the details of the other agencies.
- The total number or, if it is not reasonably practicable to work out the total number, an estimate of the total number of each of the following:
    - All individuals affected or likely to be affected by the data breach.
    - Affected individuals for the data breach.
- Either:
    - The total number of individuals notified of the data breach or, if it is not reasonably practicable to work out the total number, an estimate of the total number; or
    - If section 57 of the IP Act is relied on, the total number of individuals who would have been notified if that section had not been relied on or, if it is not reasonably practicable to work out the total number, an estimate of the total number.
- Whether the individuals notified have been advised about how to make a privacy complaint to QLeave under section 166A of the IP Act.

If it is not reasonably practicable to include all required information in the initial statement, the Manager Legal Services must take all reasonable steps to provide the information to the OIC as soon as practicable.

4.3 Exemptions to notification requirements

There are several exemptions to the mandatory data breach notification requirements, including where notification would prejudice investigations and proceedings, where QLeave has taken remedial action, notification would be inconsistent with confidentiality obligations or would compromise cybersecurity.

The Manager Legal Services will consider whether an exemption applies and consult with ITI for exemptions with respect to comprises to cybersecurity.[7]

Where an exemption relating to health or safety or cyber security is relied on, the Manager Legal Services must provide a written notice to the OIC advising of the reliance on the exemption and provide other specified information.[8] The Manager Legal Services should keep appropriate records of any assessment and decision-making process leading to reliance on an exemption.

4.4 Notification to individuals

If there is an eligible data breach and none of the exemptions apply, the Manager Legal Services must notify relevant individuals of the eligible data breach.

Specifically, the Manager Legal Services must:

- take reasonable steps to notify each individual where it is reasonably practicable to do so, where the individual's personal information has been accessed, disclosed, or lost.
- take reasonable steps to notify each affected individual, if direct notification is not practicable, but it is reasonably practicable to notify each affected individual.

Whether it is reasonably practicable will depend on a consideration of factors, including:

- the time, cost and the effort required to notify affected individuals; and
- the currency and accuracy of their contact details, which will affect the ability of the agency to notify the affected individuals.

If neither direct nor affected individual notification is practicable, the Communications team must publish the information on QLeave's accessible website for at least 12 months (provided it does not prejudice QLeave's functions). The Manager Legal Services will provide the OIC with information about how to access the notice, as soon as practicable after a public notice is published on QLeave's website. The OIC must then publish information about how to access the notice on OIC's website for at least 12 months.

The notification to individuals must, to the extent it is reasonably practicable, include the information required in s 53(2) of the IP Act (**the required information**):

- QLeave's name and, if more than one agency was affected by the data breach, the name of each other agency.
- The Manager Legal Services' contact details.
- The date the data breach occurred.
- A description of the data breach, including the type of eligible data breach.
- Information about how the data breach occurred.
- For direct or affected individual notifications:
    - A description of the personal information the subject of the data breach.
    - QLeave's recommendations about the steps the individual should take in response to the data breach.
- For public notifications:

[7] IP Act s 60

[8] IP Act ss 59(2) and 60(3).

- A description of the kind of personal information the subject of the data breach, without including any personal information in the description.
- QLeave's recommendations about the steps individuals should take in response to the data breach.

- If the data breach involved unauthorised access to or disclosure of personal information - the period during which the access or disclosure was available or made.
- The steps QLeave has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach.
- Information about how an individual may make a privacy complaint to QLeave under section 166A of the IP Act.

Legislation

- *Information Privacy Act 2009* (Qld)

Other related documents

- MDBN Assessment tool: https://oic.advancedforms.squiz.cloud/form/mandatory-notification-data-breach-mndb-scheme
- OIC Mandatory Notification of Data Breach scheme Guideline
- Information Privacy Policy and Procedure
- Right to Information Policy and Procedure

Definitions

Term	Definition
Administered legislation	QLeave's administered legislation means the: ○ *Building and Construction Industry (Portable Long Service Leave) Act 1991* ○ *Contract Cleaning Industry (Portable Long Service Leave) Act 2005* ○ *Community Services Industry (Portable Long Service Leave) Act 2020*
Eligible data breach	Where the breach involves: • Unauthorised access to, or unauthorised disclosure of personal information, which is likely to result in **serious harm** to an individual to whom the information relates. • Loss of personal information where unauthorised access to, or disclosure of information is likely to occur and if it was to occur would be likely to result in **serious harm** to an individual to whom the information relates.
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.

Term	Definition
	Determined by considering: • The kind of personal information accessed, disclosed or lost; and • The sensitivity of the personal information; and • Whether the personal information is protected by 1 or more security measures; and • If the personal information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome; and • The persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and • The nature of the harm likely to result from the data breach; and • any other relevant matter.
Individual	Means a natural person.
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.
Reasonable grounds	The High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person', it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'. As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors supporting the presence of 'reasonable grounds' should outweigh those against that conclusion.

Content Owner

For further information, please contact:

Manager Legal Services

legalservices@qleave.qld.gov.au

Version Control

Version	Effective Date	Comments
v1	01/07/2025	Creation of new separate policy and procedure to assess, manage and report on eligible data breaches, in line with the IP Act.