

Information Management Policy Framework

Policy

Data Breach

July 2025

Version 2.0

Public



Document details

Security Classification	PUBLIC					
Date of review of security classification	July 2025					
Author	Travis Hall, Records Coordinator					
Document Status	<input type="checkbox"/>	Working draft	<input type="checkbox"/>	Consultation	<input checked="" type="checkbox"/>	Final version

Document Version and Change Log

Version	Date	Prepared / Modified by	Changes	Approved by
1.0	November 2018	Records Coordinator	Final Version	The Clerk
1.0	July 2020	Records Coordinator	Reviewed – no changes made	The Clerk
1.1	September 2024	Records Coordinator	Update to Step 3 – Notifying individuals	The Clerk
2.0	March 2025	Records Coordinator	Updated to Policy. Incorporates all requirements stipulated by OIC for publishing.	The Clerk

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:
Travis Hall, Records Coordinator, Queensland Parliamentary Service

Copyright

Data Breach Policy

Copyright the Parliament of Queensland 2025

Licence



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License](https://creativecommons.org/licenses/by-nc-nd/3.0/au/). The details of the relevant license conditions are available on the Creative Commons website. Text from this publication should be attributed as Parliament of Queensland.



Acknowledgement

This document includes material from the following sources:

- **Office of the Information Commissioner (Queensland): Privacy breach management and notification**
<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification>
- **Office of the Information Commissioner (Queensland): Mandatory Notification of Data Breach scheme**
https://www.oic.qld.gov.au/_data/assets/pdf_file/0007/64294/Guideline-MNDB-mandatory-notification-of-data-breach.pdf
- **Office of the Information Commissioner (Queensland): Mandatory Notification of Data Breach scheme – Data Breach Registers and Policies**
https://www.oic.qld.gov.au/_data/assets/pdf_file/0006/64293/Guideline-MNDB-data-breach-registers-and-policies.pdf
- **Office of the Information Commissioner (Queensland): Mandatory Notification of Data Breach scheme – Exemptions**
https://www.oic.qld.gov.au/_data/assets/pdf_file/0005/64292/Guideline-MNDB-exemptions.pdf
- **Office of the Australian Information Commissioner: Notifiable data breaches**
<https://www.oaic.gov.au/privacy/notifiable-data-breaches>

Information Security

The document has been classified using the Queensland Parliamentary Service Information Security Classification (PSISC) as PUBLIC and will be managed according to the requirements of the PSISC.



Purpose

This Policy helps the Queensland Parliamentary Service (PS) to contain, mitigate, assess and respond when a data breach, or suspected data breach, has occurred. The Policy supports the PS to comply with the Mandatory Notification of Data Breach (MNDB) scheme introduced by the Office of the Information Commissioner (OIC) and assists to mitigate potential harm to affected individuals of an 'eligible data breach' (a data breach that triggers notification under the MNDB scheme).

Applicability

This Policy applies to:

- Parliamentary Service employees.
- Contractors and consultants to the Parliamentary Service.
- Electorate officers (when acting as Parliamentary Service employees).

This policy does not apply to:

- The Legislative Assembly or its Committees (including staff directly supporting them).
- Members of Parliament and their electoral office staff (when acting on behalf of the Member of Parliament).
- Statutory and portfolio Parliamentary Committees.
- Parliamentary proceedings that are kept by the Parliamentary Service.

Authority

The Speaker is afforded the authority to make and determine policies for the Parliamentary Service under section 6 of the *Parliamentary Service Act 1988*. Section 8 of the *Parliamentary Service Act 1988* then permits delegation of this authority from the Speaker to the Clerk of the Parliament. This policy is therefore made under the authority of the Clerk of the Parliament.

Review

This policy will be reviewed after 12 months initially, and then every three years thereafter.

Policy Statement

The PS is committed to compliance with the *Information Privacy Act 2009* (Qld) (IP Act), and in particular Chapter 3A of the IP Act that details the MNDB scheme.

When the PS knows or reasonably suspects that a data breach has occurred, it will:

- Immediately, and continue to take all reasonable steps to:
 - Contain the data breach.
 - Mitigate the harm caused by the data breach.
- Assess whether the data breach is an 'eligible data breach' within 30 days.
- Notify the OIC and individuals of an 'eligible data breach' as soon as practicable.
- Keep a register of all data breaches, including 'eligible data breaches'.



Policy Benefits

As the PS bears a significant responsibility to uphold robust privacy standards, complying with the MNDB provisions set out by the OIC will ensure it is:

- Demonstrating it can be trusted custodians of personal information.
- Improving transparency and accountability of its handling of personal information.
- Committed to the overarching principle of privacy.
- Increasing certainty for the community that they will be notified in the event of an 'eligible data breach'.

Policy Requirements

Policy Requirement 1: PS will take all reasonable steps to contain a data breach and mitigate the harm caused by it

The PS will take action to contain the data breach and minimise any resulting damage. For example, it will make efforts to recover the personal information¹, shut down the system that has been breached, suspend the process or activity that led to the data breach, and revoke or change access codes or passwords.

If a third party has the personal information and declines to return it, it may be necessary for the PS to seek legal advice on what action can be taken to recover the information. When recovering information, the PS will endeavour to make sure that copies have not been made, or if they have, that all copies are recovered.

The following steps have been identified and must be followed in responding to, containing, and mitigating a data breach, including appropriate escalation pathways.

1. Inform the Privacy Officer

If a data breach, or suspected data breach, has occurred, the PS staff member who discovered the data breach must notify the Privacy Officer immediately. To the best of their ability, the PS staff member should also record and advise the Privacy Officer of the time and date that the data breach was discovered, the type of personal information involved, and the suspected cause and extent of the data breach.

2. Determine if the data breach is an 'eligible data breach'

Once notified, the Privacy Officer must determine whether the data breach, or suspected data breach, that has occurred is an 'eligible data breach'. When determining if the data breach is an 'eligible data breach' the Privacy Officer must consider if:

- There has been unauthorised access to, or unauthorised disclosure of,² personal information held by the PS, or there is a loss of personal information held by the PS in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

¹ 'Personal information' is defined comprehensively in the [Privacy Policy](#).

² *Information Privacy Act 2009*, s 23; Sections 2.3.1 and 2.3.2 of the [IPOLA Guideline](#) define 'unauthorised access and disclosure'.



- The unauthorised access to, or disclosure of the information is likely to result in serious harm³ to an individual to whom the personal information relates.

If the above two points apply, then the Privacy Officer can assume that an 'eligible data breach' has occurred.⁴

3. Escalate the data breach or 'eligible data breach' to the Clerk

The Privacy Officer must immediately notify the Clerk and Deputy Clerk whenever a data breach or 'eligible data breach' has occurred, providing as much detail as possible. This should include the time and date that the data breach or 'eligible data breach' was discovered, the type of personal information involved (if any), and the suspected cause and extent of the data breach or 'eligible data breach'.

The Privacy Officer should consider each data breach on its merits, and if the Privacy Officer determines that the data breach is not an 'eligible data breach', they must still capture it in the data breach register.

4. Call a meeting of the Data Breach Response Team

Once the Privacy Officer is satisfied that an 'eligible data breach' has occurred, and they have informed the Clerk and Deputy Clerk, a meeting of the Data Breach Response Team must be called. The Data Breach Response Team should undertake the following (as required) to contain the 'eligible data breach':

- Ensure ITS implements the Cyber Security Incident Response Plan (where applicable).
- Notify building security (where applicable).
- Advise the relevant information system administrators (e.g., Aurion, Objective, TechOne, etc).
- Gather evidence to assist with determining the cause of the 'eligible data breach'.
- Recover the breached data or information (if possible).
- Inform the Clerk, Deputy Clerk and ELT as soon as possible and provide ongoing updates on key developments.

Policy Requirement 2: PS will assess every suspected data breach to determine if it is an 'eligible data breach'

If the PS reasonably suspects that a data breach is an 'eligible data breach', it must assess whether there are reasonable grounds to confirm those suspicions. The assessment must be completed within 30 days unless the assessment time is extended.

The PS's assessment and reasons for its decision as to whether a data breach is an 'eligible data breach' should be recorded in the [Data Breach Reports and Investigations](#) file in Objective.

When conducting an assessment, the PS should evaluate the priorities and risks by collecting information about the data breach, including:

- Date, time, duration, and location of the data breach.
- Type of personal information involved in the data breach.
- How the data breach was discovered and by whom.
- The cause and extent of the data breach.
- A list of the affected individuals, or possible affected individuals.
- The risk of serious harm to the affected individuals.

³ *Information Privacy Act 2009*, sch 5; Section 2.4.1 and 2.4.2 of the [IPOLA Guideline](#) define 'likely to result' and 'serious harm'.

⁴ [Policy Requirement 2](#) assists to thoroughly and accurately assess suspected data breaches.



- The cause and extent of the data breach.

If the PS is unable to complete the assessment in 30 days, it can request from the OIC to extend the 30 days by a further period that is reasonably required to complete the assessment.

If the PS becomes aware that a breach may affect another agency, it will give written notice to those agencies that includes the following information:

- A description of the data breach.
- A description of the kind of personal information that is the subject of the data breach, without including any personal information in the description.

If all the personal information that is subject to the PS data breach is also the subject of the data breach of another agency, and that agency has undertaken to conduct a data breach assessment, the PS is not obliged to conduct its own assessment.

The following questions have been identified to assist the PS to thoroughly and accurately assess suspected data breaches.

1. What type of personal information is involved?

Some types of personal information are more likely to cause an individual harm if it is compromised. For example, Medicare numbers, driver's licence numbers, health information, credit card numbers and tax file numbers, are more significant than names and email addresses. A combination of personal information creates greater potential for harm than a single piece of personal information.

2. Who is affected by the data breach?

Who, and how many, has been affected by the data breach? Do any of these people have personal circumstances which may put them at any particular risk or harm?

3. What was the cause of the data breach?

Did the data breach occur as part of a targeted attack or through inadvertent oversight? Was it a one-off incident or does it expose a more systemic vulnerability? Has the personal information been recovered? Is the personal information encrypted or otherwise not readily accessible?

4. What is the foreseeable harm to the affected individuals?

What possible access, use or disclosure is there for the personal information? Where information is stolen, suspected intent to harm raises the need to comply with the PS's notification obligations.

Policy Requirement 3: PS will notify the OIC and all affected parties when an 'eligible data breach' occurs

If the PS determines there has been an 'eligible data breach' it must prepare a statement for the OIC and notify any individuals affected by the data breach.

1. Notifying the OIC

The PS must prepare and give the OIC a statement, which must include:

- The PS's details and, if more than one agency was affected by the data breach, the name of any other agency.
- Whether the PS is reporting on behalf of other agencies affected by the same data breach and, if so, the details of the other agencies.



- The contact details of the Privacy Officer, as the nominated staff member to be contacted in relation to the data breach.
- The date the data breach occurred (if known).
- A description of the 'eligible data breach'.
- A description of the kind of personal information involved in the data breach, without including any personal information in the description.
- 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 the PS has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach.
- The PS's recommendations about the steps individuals should take in response to the data breach.
- The total number or, if it is not reasonably practicable to work out the total number, an estimate of the total number of individuals whose personal information was accessed, disclosed or lost and affected individuals for the data breach.
- Whether the notified individuals have been advised how to make a privacy complaint to the PS.
- 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.

If it is not reasonably practicable to include some of the above information to the OIC (e.g. the PS may not yet know the total number of affected individuals) the PS must take all reasonable steps to provide required information to the OIC as soon as practicable.

2. Notifying individuals

When an 'eligible data breach' occurs, individuals impacted by the data breach must be notified. In the first instance the PS must take reasonable steps to notify everyone whose personal information was accessed, disclosed or lost if reasonably practicable.

If that is not possible, the PS must take reasonable steps to notify each affected individual, if reasonably practicable⁵.

If personal notifications identified above are not possible, the PS must publish relevant information on its website for at least 12 months and must advise the OIC and they will also publish it for 12 months.

When notifying individuals, the following information should be provided:

- PS contact details.
- Date the breach occurred.
- Description of the breach (how it occurred and length of exposure).
- Details of the containment and mitigation steps taken by the PS.
- Steps the individual can take in response to the breach to protect themselves from harm.
- Complaint rights.⁶

However, if a data breach is not deemed to be an 'eligible data breach' there are occasions where notification can be counterproductive. For example, notifying individuals about a data breach which is

⁵ 'Affected individual' is someone to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach: *Information Privacy Act 2009*, ss 47(1)(a)(ii) and 47(1)(b0(ii)).

⁶ *Information Privacy Act 2009*, sch 3, pt 5.



unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a more significant breach.

Factors to consider when deciding whether notification is appropriate include:

- What is the risk of harm to the individual?
- What steps has the PS taken to avoid or remedy any actual or potential harm?
- What is the ability of the individual to take further steps to avoid or remedy harm?
- Is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
- Are there any applicable legislative provisions or contractual obligations that require the PS to notify affected individuals?
- Is the risk of notification to an individual likely to cause more harm than the risk posed by the data breach?

If notification is deemed appropriate, the PS should notify individuals or organisations affected by the data breach as soon as practical. The PS may also delay notification if the investigation of the data breach could be compromised, or a software vulnerability may be revealed.

If notification of individuals is deemed inappropriate in the circumstances the reasons for that decision should be recorded in the data breach register.

Policy Requirement 4: PS will keep an internal register of all data breaches

Maintaining a data breach register will contribute to accurate recordkeeping and reporting processes. Data from the register will also assist with tracking and analysing data breach risks and reviewing the efficacy of the PS's response methods. The information will also assist the PS in responding to requests for information from the OIC.

The register must include the following information:

- A description of the data breach, whether the breach is an 'eligible data breach' or not.
- Action taken by the PS staff member/s and/or Privacy Officer to contain the data breach and mitigate its harm.
- The Privacy Officer's reasons for determining whether the data breach was an 'eligible data breach' or not.
- The date the PS gave a statement to the OIC about the 'eligible data breach' and the date any additional information was provided.
- The individuals who were notified and the date and method by which they were notified (if applicable).
- Details of any notification exemption.
- Details of the actions taken by the PS to prevent future data breaches of a similar kind occurring.



Definitions

<i>Term</i>	<i>Definition</i>
Data breach	The unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information.
Data Breach Response Team	PS roles with the relevant skills needed to respond to a data breach. Each data breach may have a different response team depending on the nature of the data breach. However, the base team includes the Director Information Services, the Privacy Officer, Head of IT, the Information Asset Custodian of the breached data, the Manager P&C and a representative from Communication & Marketing. Other PS roles and external parties are invited depending on the nature of the breach.
Eligible data breach	Both of the following must apply for a data breach to be an 'eligible data breach': <ol style="list-style-type: none"> 1. There is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and 2. The unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual').
Information Asset Custodian	The organisation or person with physical custody or delegated responsibility of the information asset. Custody does not indicate legal responsibility for, or ownership of, the information.
Information Asset Manager	The PS role with practical day-to-day responsibility for the information asset.



Appendix 1

What is a data breach?

A data breach is the unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information.

Data breaches can result from technical issues, human error, inadequate policies and training, a misunderstanding of the law, or deliberate acts. A common cause of data breaches is when personal information is lost, stolen or mistakenly disclosed. Common data breach examples include:

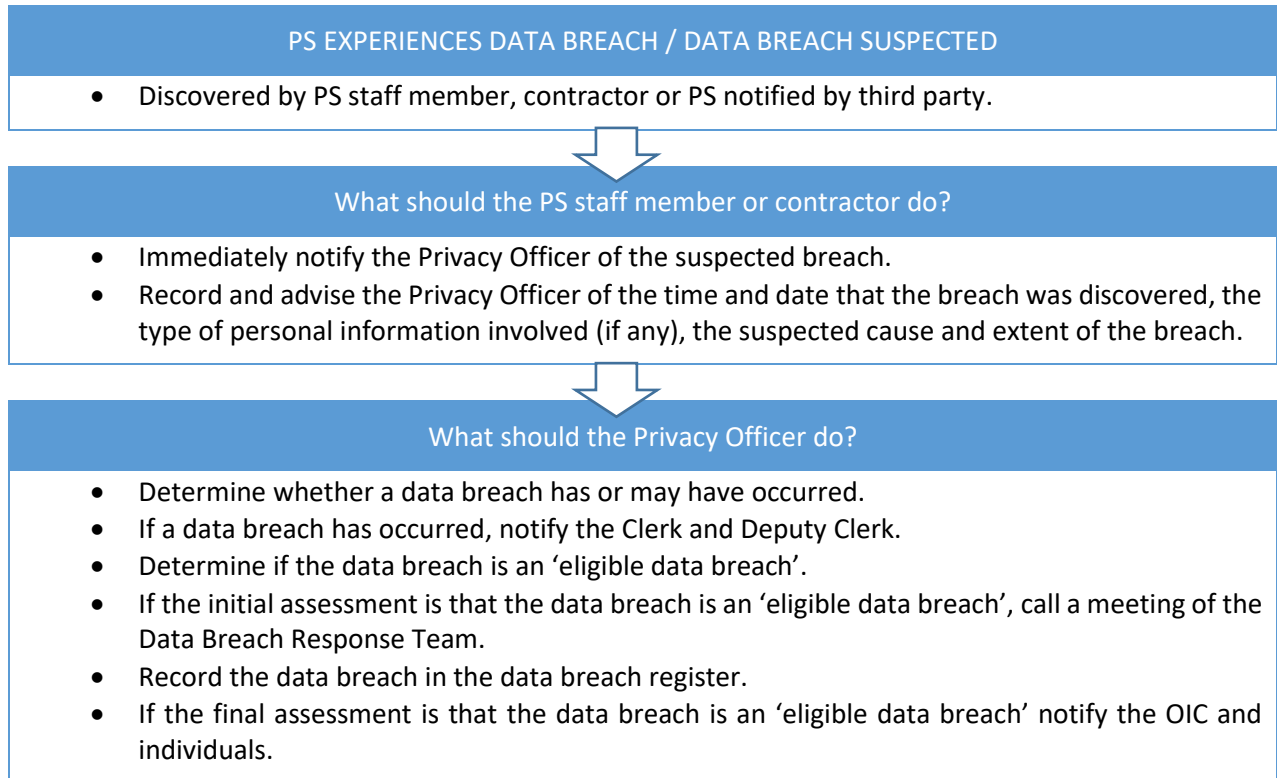
- A folder containing emergency staff contacts is lost.
- An email is sent to unintended recipients.
- A staff member's smart phone, containing contact details and business emails, is stolen.
- A PS laptop is left unattended, and the personal information is seen by family members.
- Confidential information is accidentally published to the website instead of the intranet.
- Personal information on the PS network is accessed by a hacker.
- Personal information stored 'in the cloud' is insufficiently secured and accessed by unintended third parties.



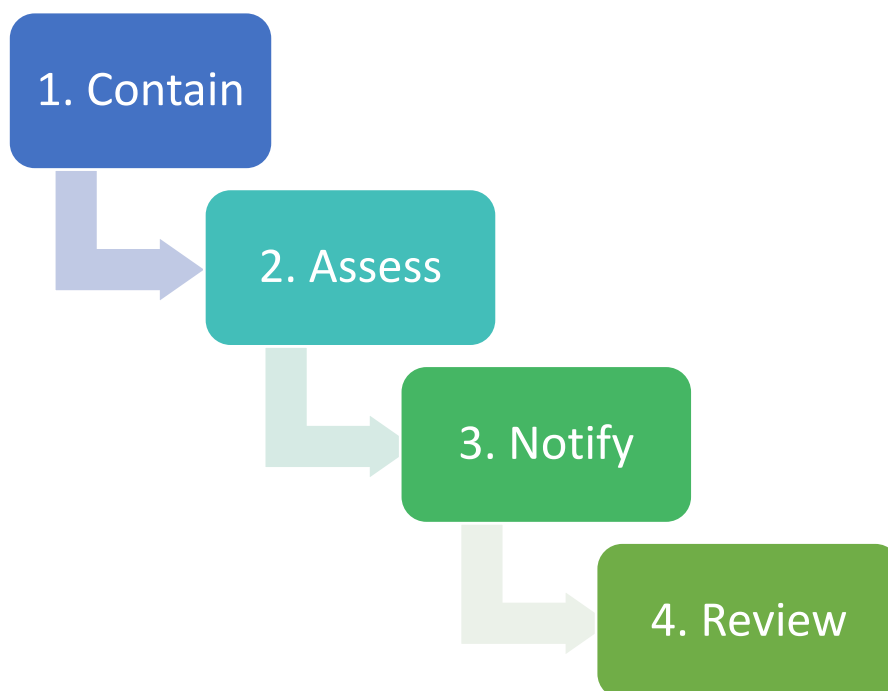
Appendix 2

Managing a data breach

1. Data breach escalation



2. Data breach response



Contain the data breach

Take action to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the process or activity that led to the privacy breach, revoke or change access codes or passwords.

If a third party has the personal information and declines to return it, it may be necessary to seek legal advice on what action can be taken to recover the information. When recovering information, make sure that copies have not been made or, if they have, that all copies are recovered.

What should be done immediately to contain the data breach?

- Notify the Privacy Officer, who in turn will notify the Clerk and Deputy Clerk and call the data breach response team.
- Immediately contain and mitigate the breach (check below as required):
 - ITS implements the ICT Incident Response Plan (where applicable).
 - Notify building security (where applicable).
 - Advise information systems' administrators.
- Gather evidence to assist with determining the cause of the breach.
- Recover the breached data or information (if possible).
- Inform the ELT as soon as possible, provide ongoing updates on key developments.

Assess the risks

Some types of personal information are more likely to cause an individual harm if compromised. For example, Medicare or driver's licence numbers, health information, credit card and tax file numbers, are more significant than names and email addresses. A combination of personal information creates greater potential for harm than a single piece of personal information.

How to assess risks from the data breach?

- Conduct an initial investigation, and collect information about the breach promptly, including:
 - Date, time, duration, and location of the breach.
 - Type of personal information involved in the breach (if any).
 - How the breach was discovered and by who.
 - The cause and extent of the breach.
 - A list of the affected individuals, or possible affected individuals.
 - The risk of serious harm to the affected individuals.
 - The risk of other harms.
- Establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.



When to notify

The PS should develop a plan of who should be notified, to what extent, and in what order, of the existence a breach.

Who will be notified and what shall be said about the data breach?

- Decide who to contact about the breach (internally, and externally) at the preliminary stage.
- Does the breach trigger the requirements of the MNDB scheme from the OIC?
- If it is not considered an 'eligible data breach' would notifying the individuals be appropriate?
- How will affected individuals be notified?
- Should other entities be notified? e.g., Members, Electorate Offices, Police, QG Cyber Security Unit, other QG agencies or organisations affected by the breach.
- Does the breach involve tax file numbers? If so, there are additional reporting requirements under the Privacy Act (Commonwealth) 1988.

Review and learn

Once the breach has been contained, investigate the circumstances of the breach to determine the cause and consider any short or long-term measures that could prevent a reoccurrence.

How will a similar data breach be prevented in the future?

- Fully investigate the cause of the breach.
- Identify and address any weaknesses in data handling that contributed to the breach.
- Conduct a post-breach review and report on outcomes and recommendations:
 - Make appropriate changes to policies, procedures and contracts.
 - Revise staff training practices.
 - Update security and response plan.

