Queensland Police Service

Data Breach Policy

Queensland Government

Creative Commons

Document Control

Role	Title
Document owner	Executive Director Legal Division or authorised delegate
Document author	Principal Privacy Officer
Document Reviewer	Director, Right to Information and Privacy Services
Document Controller	Principal Privacy Officer

Document History

Date	Version	Author	Comments and amendments
31 May 2025	1	Principal Privacy Officer	Initial draft
10 June 2025	2	Director RTIPS	Minor amendments
23 June 2025	3	Principal Privacy Officer	Creative Commons attribution added
23 June 2025	FINAL	Principal Privacy Officer	FINAL

Contents

1. Introduction

The Queensland Police Service (QPS) is an agency to which the provisions of the *Information Privacy Act 2009* (IP Act) apply. The object of the IP Act is to provide for the fair collection and handling of personal information in the Queensland public sector.

Chapter 3A of the IP Act establishes the Mandatory Notification of Data Breach (MNDB) scheme. The MNDB scheme requires agencies to notify the Information Commissioner and affected individuals of eligible data breaches, unless an exception applies. Agencies, including the QPS are required to prepare and publish a Data Breach Policy (this Policy) and to keep a register of eligible data breaches. The Policy is required to set out how the QPS will respond to a data breach, including a suspected eligible data breach.

2. Purpose and scope

This Policy applies to all QPS members, as defined by the *Police Service Administration Act 1990* (PSA Act) including contracted service providers as defined by Chapter 2, Part 3 of the IP Act.

The purpose of this Policy is to provide guidance to QPS members on the handling of data breaches in relation to personal information held by the QPS. The QPS is responsible for a considerable amount of sensitive, confidential personal information and the unauthorised disclosure, access or loss of such information could significantly impact affected individuals. The safety and privacy of individuals affected by domestic and family violence (DFV) and other vulnerable persons is of critical importance. Any unauthorised disclosure of their personal information may pose risks of serious harm to affected individuals.

While not every data breach will be an eligible data breach the QPS remains committed to the proper management of all breaches involving personal information.

This Policy sets out:

- What constitutes an eligible data breach under the IP Act
- The key stages involved in the QPS' preparation for, and response to a data breach including post-breach review and evaluation
- The roles and responsibilities of QPS members with assigned functions under the Policy

3. Data Breach and Eligible Data Breach under the IP Act

A **data breach** is defined in the IP Act as an unauthorised access or disclosure of information held by an agency, or the loss of information held by an agency where unauthorised access or disclosure is likely to occur. A data breach may or may not involve personal information. For example, statistics or financial data could be the subject of a data breach but that data may not necessarily include personal information. For the purposes of this policy when a data breach is referred to it means a data breach that involves the unauthorised access, loss or disclosure of data that includes personal information.

A data breach isn't limited to the unauthorised disclosure of personal information outside the QPS. For example, unauthorised access to personal information by a QPS member, or

unauthorised sharing of personal information between divisions within the QPS may amount to a data breach.

An **eligible data breach** occurs where a data breach involves the loss or unauthorised access or disclosure of personal information which is likely to result in *serious harm* to an affected individual.

Identification and assessment of a data breach and an eligible data breach is dealt with in the context of responding to a data breach in six key stages.

4. Responding to a data breach – six key stages

Each suspected data breach or suspected eligible data breach must be considered on a case by case basis, with an understanding of the risks posed by the breach (to the extent possible based on the information available) and the actions that would be most effective in reducing or removing these risks. This policy identifies the six key stages undertaken by the QPS in preparing for and responding to a data breach. At any time throughout the key stages the QPS should take remedial action where possible to limit the impact of the breach on affected individuals. Depending on the nature of the breach it may be appropriate to combine steps or to move between stages in quick succession. The QPS is committed to treating all suspected or actual data breaches seriously, promptly moving to contain, assess and remediate the incident.

Stage 1 – Preparation

The QPS has implemented a comprehensive framework of data security policies, service manuals, awareness initiatives and training programs designed to reinforce best practice for authorised information disclosure with the intention of avoiding the mishandling of personal information.

Training requirements

All QPS members must complete the following online learning products (OLP):

- **Information Privacy OLP** (Privacy Unit): Provides guidance on QPS' statutory obligations under the IP Act and outlines the role of QPS members in supporting compliance and minimising privacy risks through responsible information handling.
- **Accessing QPS information OLP** (Ethical Standards Command): Covers authorised access and disclosure of QPS information emphasising accountability and potential disciplinary actions resulting from unauthorised handling of confidential or personal information.
- **Cyber security awareness OLP** (Cyber Security, Frontline Digital Division): Addresses information security emphasising mitigation of risk of security events through improved awareness of phishing and other potential cyber security social engineering threats.

Service policies and manuals

QPS members are required to adhere to service manuals, policies and procedures to ensure consistency, accountability and compliance with relevant legislative obligations. Relevant resources include:

- Management Support Manual
- Operational Procedures Manual
- Digital Electronic Recording of Interviews and Evidence Manual

These resources provide:

- Clear operational standards that outline expectation for professional conduct
- Legislative alignment, ensuring duties are performed in accordance with the IP Act and other applicable laws
- Decision making frameworks that support ethical and lawful information handling.

The suite of QPS ICT policies and procedures reflects requirements specified in the Queensland Government Information Security Policy 18 (IS18) and ISO/IEC 27001, the international standard to manage information security.

Stage 2 – Identification

Refer to item 3 of this policy which sets out the definition of **data breach** and an **eligible data breach.**

A possible data breach could be identified in several ways, for example:

- **System activity monitors** – identification of unusual system activity and unauthorised access attempts.
- **Reports from system users or employees** – identification of correspondence sent to the wrong recipient through quality assessment reviews or a contractor may identify that shared information exceeds the limits of the contracted service.
- **Reports from members of the public** – a recipient of correspondence may identify they were not the intended recipient or were provided with the personal information of another individual.

An agency may suspect that a data breach has occurred when unauthorised access, disclosure or loss (which may result in unauthorised access or disclosure) is identified. Human error accounts for the majority of data breaches that involve the mishandling of personal information. The following are examples of scenarios which may give rise to a suspicion (or a reasonable belief) that a data breach has occurred:

Unauthorised Access	Unauthorised Disclosure	Loss
An employee browses agency records relating to a family member, neighbour or celebrity without a legitimate purpose.	An agency intended to send only de-identified information to a researcher. In error information with personal identifiers was provided.	An agency sells a laptop or a filing cabinet that contains an individual's personal information.
Agency data is compromised during a cyberattack and intentionally accessed by a threat actor.	An agency employee discloses personal information to a third party who is not the intended recipient.	An agency employee accidentally leaves an unencrypted USB, that is not password protected, that contains personal information on public transport.
An employee is given access to a database as part of a project. The employee continues to access the	A database hosted in a cloud or web facing environment does not have appropriate access controls and the data	A device is lost but believed to be destroyed or inaccessible – a data breach is unlikely (e.g. documents

documents after their involvement with the project has ceased.	is visible to and accessed by unauthorised individuals.	destroyed in a natural disaster or a lost password protected laptop is recovered with no evidence of access).

Reporting a suspected data breach to the Privacy Unit

Suspected data breaches should be escalated to a supervisor then immediately reported to the Privacy Unit.

A **Privacy Breach Notification** form is located on the Privacy Unit SharePoint site to assist in prompt reporting of suspected data incidents.

Notification can also be made by email directly to the Privacy Unit (privacy@police.qld.gov.au). A Privacy Officer will provide the reporting supervisor with a Privacy Breach Notification form for completion. After conducting a preliminary assessment the Principal Privacy Officer may convene the Data Breach Response Team in accordance with Frontline and Digital Division protocols.

Members of the public can report suspected data breaches directly to the QPS Privacy Unit by email - privacy@police.qld.gov.au.

Stage 3 – Containment and mitigation

When the QPS knows, or reasonably believes a data breach is an eligible data breach it must immediately take, and continue to take all reasonable steps to:

- contain the data breach and
- mitigate the harm caused by the data breach

The Privacy Unit, in consultation with relevant internal stakeholders will determine the appropriate containment strategies taking into consideration:

- the cause of the incident
- the seriousness of the incident (what information and individuals are impacted)
- whether interim controls can be implemented
- if the information has been incorrectly disclosed, can the recipient be contacted and the material recovered
- can the system which has been breached be shut down
- can the activity which led to the breach be stopped
- can the access codes or passwords be changed
- whether the breach occurred due to an external cyber incident

If the suspected breach involves other government agencies:

- document key external agency contacts
- define roles and responsibilities for assessment and remediation, information flow and,
- procedures and responsibilities for notification to individuals and the Information Commissioner

Stage 4 – Assessment

When the QPS *reasonably suspects* the breach is an eligible data breach an assessment must be conducted to determine whether there are reasonable grounds to support this. The assessment will be conducted by the Privacy Unit with the assistance of relevant business areas.

Refer to item 3 of this policy which sets out the definition of **data breach** and an **eligible data breach.**

What is 'serious harm'?

The harm that could arise from a data breach will vary based on the nature of the personal information and the context of the breach.

Serious harm is defined in the IP Act as including –

- serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure or
- serious harm to the individual's reputation because of the access or disclosure

Serious harm occurs when the harm arising from the data breach has or may result in a real and substantial detrimental effect on the individual. The effect must be more than mere irritation, annoyance or inconvenience.

What is 'likely to result'?

The risk of harm must be more than merely possible. It must be more probable than not to occur. Whether a data breach is likely to result in serious harm is an objective test taking the facts of the specific breach into account including the matters set out in s47(2) of the IP Act.

Section 47(2) factors

When determining whether the data breach may result in serious harm to an individual the following matters must be taken into account:

- the kind of personal information accessed, disclosed or lost
- the sensitivity of the personal information
- whether the personal information was protected by 1 or more security measures
- if the personal information is protected by 1 or more security measures – the likelihood that any of those security measures could be overcome
- the persons or kinds of persons who have obtained or who could obtain the personal information
- the nature of the harm likely to result from the data breach
- any other relevant matter

Determining what a 'relevant matter' may be will depend on the nature of the breach but the following may assist in determining the seriousness of the breach:

- the nature of the breach
- is it likely a third party caused the breach?
- is another agency involved?
- Are there any vulnerabilities of the affected individuals? (children or DFV survivor)
- How effective has containment been? Has the mitigation lessened the risk?

Stage 5 – Notification

Subject to the outcome of the data breach assessment the QPS may be required to notify the Information Commissioner, affected individuals or other agencies. The Privacy Unit will coordinate notification of the OIC and individuals on behalf of the QPS. The type of notification will be dependent upon the size of the breach, in accordance with the provisions of the IP Act.

Notifying the Office of the Information Commissioner

As soon as practicable after forming a reasonable belief that a data breach is an eligible data breach the QPS must provide the Information Commissioner with a statement which addresses the matters in s51(2) of the IP Act, unless an exemption applies.

Notification of an eligible data breach will include:

- whether the QPS is reporting on behalf of other agencies affected by the same data breach and if so, the details of the other agencies
- the date the data breach occurred (if known)
- 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 QPS has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach
- QPS' recommendations about the steps affected individuals should take in response to the data breach
- the number of individuals whose personal information was accessed, disclosed or lost and affected individuals for the data breach
- 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
- whether the notified individuals have been advised how to make a privacy complaint to QPS

Notifying affected individuals

As soon as practicable after forming a reasonable belief that a data breach is an eligible data breach the QPS must also notify individuals affected by the breach, unless an exception applies.

The Privacy Unit will coordinate notification of individuals on behalf of the QPS.

Notification of an eligible data breach to affected individuals will include:

- the contact details of QPS or a person nominated by QPS for further queries about the data breach
- the date the data breach occurred (if known)
- a description of the data breach
- information about how the data breach occurred
- QPS' recommendations about the steps an affected individual 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 QPS has taken or will take to contain the data breach and mitigate any harm caused to affected individuals
- information about how an individual can make a formal privacy complaint.

The method of notification will be determined on a case by case basis in accordance with the provisions of the IP Act.

Public Notifications

The Public Notifications page, located on the QPS website (www.police.qld.gov.au) contains the details of the public notification of an eligible data breach under s53(1)(c) of the IP Act. A public notification is provided when it is not reasonably practicable to directly notify any or all of the individuals affected by an eligible data breach.

A list of all public notifications made by QPS is located in the Public Notifications page. The QPS will retain notifications in the register for a period of at least 12 months in accordance with the IP Act.

Stage 6 – Post data breach review and remediation evaluation

After resolution of the data breach a post breach review may be conducted on:

- the cause of the data breach
- assets and controls impacted and identification of improvements
- policies and procedures to incorporate insights and knowledge gained as a result of the data breach
- opportunities to provide tailored privacy training

5. Recordkeeping

The QPS makes and retains records, including records in connection with data breaches, in accordance with its obligations under the *Public Records Act 2023*. The QPS also maintains an internal register of eligible data breaches as required by s72 of the IP Act.

6. Related legislation and policies

- QPS Management Support Manual
- QPS Operational Procedures Manual
- QPS QPP Privacy Policy
- *Police Service Administration Act 1990*
- *Police Powers and Responsibilities Act 2000*

7. Roles and responsibilities

Role	Responsibilities
Commissioner of the Queensland Police Service (Commissioner)	The Commissioner is responsible for the efficient and proper administration management and functioning of the police service, pursuant to the provisions of the *Police Service Administration Act 1990* including information management

	activities of the QPS and to ensure that the personal information under the control of QPS accords with the obligations under the IP Act.
Information owner	The person identified as having the authority and accountability for one or more of the relevant information assets.
Managers and supervisors	Managers and supervisors are responsible for taking immediate steps to ensure QPS' Data Breach Form is completed and forwarded to the Privacy Unit for assessment, and to notify the relevant Information owner and any other relevant parties. This list is not exhaustive and any business area within QPS may be a relevant party.
Employees, consultants, contractors and managed service providers	All employees, consultants and contractors are responsible for: • recognising a data breach and promptly reporting it • only collecting or using personal information in accordance with QPS' QPP policy • restricting access to information only to those who require it for their role • only keeping information for the length of time necessary in accordance with the retention and disposal schedules • understanding their obligations under all relevant legislation, policies, procedures and guidelines, including the *Code of Conduct for Queensland Public Service*, and the *Police Service Administration Act 1990* and by completing the mandatory information privacy, cyber security and ESC training.
Frontline and Digital Division (F&DD)	F&DD manages and maintains QPS' obligations regarding compliance with the Queensland Government Information Security Policy IS18 ▪ notifying the Privacy Unit where an actual or suspected breach may involve personal information. ▪ assist with the appropriate and necessary containment measures, root cause eradication and post breach review. ▪ providing guidance and training to QPS members on best practice for cyber security.
Privacy Unit	The Privacy Unit manage the assessment, and coordinate containment and notification as required for all data

	breaches that include personal information and are responsible for: ▪ assessment of data breaches containing personal information ▪ notification forms and templates, and central breach register that will be used to manage and record details of the incident ▪ co-ordinating notification of an eligible data breach to the OIC and affected individuals ▪ educating employees about data breaches and recommending improvement to processes that will reduce the risk of future incidents ▪ reviewing and updating QPS' QPP Policy and this Data Breach Policy.
Ethical Standards Command (ESC)	The Ethical Standards Command is responsible for investigating an incident to determine whether serious misconduct or corrupt conduct has occurred.

8. Definitions

Personal information (Section 12 of the IP Act)

Personal information means 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.

Data breach (Schedule 5 (Dictionary) of the IP Act)

data breach, of an agency, means either of the following in relation to information held by the agency—

(a) unauthorised access to, or unauthorised disclosure of, the information;

(b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

Eligible data breach (Section 47 of the IP Act)

(1) An ***eligible data breach*** of an agency is a data breach of the agency that occurs in relation to personal information held by the agency if—

(a) both of the following apply—

(i) the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information;

(ii) the access or disclosure is likely to result in serious harm to an individual (an ***affected individual***) to whom the personal information relates, having regard to the matters stated in subsection (2); or

(b) the data breach involves the personal information being lost in circumstances where—

(i) unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and

(ii) if the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual (also an ***affected individual***) to whom the personal information relates, having regard to the matters stated in subsection (2).

(2) For subsection (1)(a)(ii) and (b)(ii), the matters are—

(a) the kind of personal information accessed, disclosed or lost; and

(b) the sensitivity of the personal information; and

(c) whether the personal information is protected by 1 or more security measures; and

(d) if the personal information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome; and

(e) the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and

(f) the nature of the harm likely to result from the data breach; and

(g) any other relevant matter.

Sensitive information (Schedule 5 (Dictionary) of the IP Act)

sensitive information, for an individual, means the following—

(a) information or an opinion, that is also personal information, about the individual's—

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

(b) health information about the individual;

(c) genetic information about the individual that is not otherwise health information;

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.