July 2026

Data Breach Policy

Information Privacy Act 2009 (Qld)

QUEENSLAND Family & Child Commission

Queensland Government

Data Breach Policy

1. Purpose, Scope and Objective

This Data Breach Policy has been developed in accordance with the *Information Privacy Act 2009* including the Mandatory Notification of Data Breach (MNDB) scheme, which requires Queensland public sector agencies to prepare and maintain a data breach policy outlining how they identify, assess and respond to data breaches, including suspected Eligible Data Breaches.

Under the *Information Privacy Act 2009*, a data breach involves unauthorised access to, or disclosure of, information or the loss of information where unauthorised access or disclosure is likely to occur.

Purpose

The purpose of this Policy is to establish the Queensland Family and Child Commission's (the Commission) approach to managing data breaches to minimise harm to individuals, ensure compliance with legislative obligations, and support timely and appropriate notification to affected individuals and the Office of the Information Commissioner (OIC).

Roles and responsibilities, breach identification and classification and governance requirements with detailed procedures set out in the Commission's Data Breach Response Plan.

Scope

This Policy applies to all actual, suspected or potential data breaches involving information held by, or on behalf of, the Commission, including information held by contracted service providers and third parties. Where a breach does not involve personal information, it will be managed by Governance and Risk and IT Services, in conjunction with the relevant business area, under applicable information security, risk management and breach response processes.

Objective

This Policy establishes the Commission's framework for managing data breaches, including governance, roles and responsibilities, breach identification and classification, assessment, notification, recordkeeping and continuous improvement.

2. Principles

The Commission is committed to:

- protecting the information it holds
- respecting individuals' right to privacy in their interactions with the Commission
- complying with the *Information Privacy Act 2009 (Qld)* and MNDB scheme requirements
- minimising harm to individuals affected by data breaches
- empowering officers to lawfully manage and protect information through mandatory training, clear reporting pathways and robust data breach management processes.

3. Policy Statement

The Commission is committed to managing data breaches in a timely and effective manner, including notifying individuals and relevant authorities as soon as practicable where a breach is assessed as an Eligible Data Breach. The Commission adopts a structured approach to managing data breaches, underpinned by the following six stages:

1. **Preparation:** establishing and maintaining controls, processes and capability to support effective data breach management.
2. **Identification:** detecting, reporting and escalating actual, suspected or potential data breaches.

3. **Containment and mitigation:** taking immediate action to limit impact, prevent further exposure and reduce the risk of serious harm.
4. **Assessment:** determining the scope, cause, impact, risk of serious harm and legislative obligations associated with the breach.
5. **Notification:** managing mandatory and voluntary notifications in accordance with legislative requirements and approved decision-making pathways.
6. **Post-incident review and remediation:** identifying lessons learned, addressing root causes and implementing improvements to prevent recurrence.

All actual, suspected or potential data breaches must be reported immediately and managed in accordance with this Policy and the Data Breach Response Plan.

Where a data breach involves a third party or service provider, the Commission remains responsible for managing the breach in accordance with the *Information Privacy Act 2009 (Qld)*, including determining whether the breach constitutes an Eligible Data Breach and meeting any applicable notification obligations.

The Commission will ensure that appropriate controls are in place to support the secure sharing of information with external agencies and partner organisations.

Where personal information is shared with other agencies, the Commission will take reasonable steps to:

- protect the information from unauthorised access, disclosure or loss
- ensure information is shared in accordance with legislative, regulatory and policy requirements
- manage risk arising from inter-agency data sharing arrangements.

Data sharing arrangements will be supported by appropriate governance, contractual controls and, where applicable, secure systems and platforms.

These stages represent the overarching framework for managing data breaches and are supported by the response process outlined in **Section 3.1**.

3.1 Data Breach Response Process

The Commission follows a structured response process to manage data breaches, aligned to the data breach management framework outlined above. The following elements describe the key components of this process, which may occur concurrently or iteratively depending on the nature of the breach.

3.1.1 Identification

The Commission ensures suspected data breaches are promptly identified and reported through established channels.

3.1.2 Containment

The Commission takes immediate action to contain the breach and prevent further unauthorised access, disclosure or loss of information.

3.1.3 Internal Notification

Relevant internal stakeholders, including Governance and Risk and IT Services, are notified in a timely manner to support a coordinated response and enable appropriate escalation where required.

3.1.4 Classification

Data breaches are triaged and classified to determine their nature (e.g. cyber security incident or other data breach type), whether personal information is involved, the potential risk of harm, and whether escalation or activation of response arrangements is required.

3.1.5 Assessment

The Commission undertakes a structured assessment of the data breach, including consideration of the sensitivity of the information, the number of individuals affected, the likelihood of misuse, and the risk of serious harm, to determine whether it meets the criteria of an Eligible Data Breach, with detailed assessment criteria and guidance provided in the Data Breach Response Plan.

3.1.6 Response

The Commission responds to the data breach in accordance with the Data Breach Response Plan. This includes implementing appropriate containment, remediation, and recovery actions, addressing root causes, strengthening controls, and supporting affected individuals where required.

3.1.7 Review and Remediation

Following resolution, the Commission reviews the incident to identify root causes, control gaps, and lessons learned, and implements improvements to policies, processes, systems, and training.

3.2 MNDB Scheme Requirements

The Commission must assess whether there are reasonable grounds to believe a data breach is an Eligible Data Breach within 30 days of becoming aware of the breach.

- immediately take all reasonable steps to contain and mitigate the data breach
- assess, within 30 days of becoming aware of the breach, whether there are reasonable grounds to believe it is an **Eligible Data Breach**
    - A data breach is considered to be eligible where there are reasonable grounds to believe that:
        - personal information has been subject to unauthorised access, unauthorised disclosure, or loss in circumstances where unauthorised access or disclosure is likely to occur; and
        - the breach is likely to result in serious harm to an individual to whom the information relates.
- document the assessment, decision-making and any reasons for applying an exemption
- notify other affected agencies, where applicable
- notify the Office of the Information Commissioner (OIC) and affected individuals as soon as practicable where the breach is confirmed as an **Eligible Data Breach**, unless an exemption applies.

Further information on contacting the Commission or making a privacy complaint is provided in **Section 3.3**.

3.2.1 Examples of Personal Information

Examples of personal information may include full name, date of birth, residential address, email address, phone number, financial or health information. Information is considered personal information where an individual can be reasonably identified from the information, either alone or in combination with other information.

3.3 Contact and Complaints

Individuals who believe their personal information has been involved in a data breach, who have been notified of a data breach, or whose parent, guardian or authorised representative is acting on their behalf, may contact the Commission using the details provided in the notification or available on the Commission's website.

Individuals may also make a privacy complaint to the Commission regarding the handling of their personal information. Where an individual is not satisfied with the outcome, they may refer the complaint to the Office of the Information Commissioner (OIC).

3.4 Examples of Eligible Data Breaches

Examples may include:

- cyber incidents (e.g. phishing, malware, hacking) resulting in unauthorised access to systems or data
- inappropriate internal access to personal information
- accidental public exposure of systems or databases
- loss or misplacement of records containing personal or sensitive information
- unauthorised disclosure of information by contractors or third parties.

4. Roles and Responsibilities

Governance and Risk, within Corporate Services, is the policy owner and is responsible for maintaining this Policy, including its ongoing suitability, legislative compliance and periodic review.

Role	Responsibilities
Principal Commissioner/ Chief Operating Officer/ Executive Directors	Provide organisational oversight and accountability for data breach management, including ensuring compliance with this Policy, promoting timely reporting and escalation, and endorsing key response and notification decisions for high-risk or notifiable data breaches where required.
Transformation, Governance & Change (TGC)	Oversee data breach management and privacy obligations, including advising on legislative requirements under the *Information Privacy Act 2009 (Qld)*, supporting assessment and escalation, maintaining this Policy and the Data Breach Response Plan, and advising on notification requirements and exemptions. Coordinate and issue notifications to affected individuals and the Office of the Information Commissioner (OIC) in accordance with legislative requirements, following endorsement through the Commission's governance arrangements.
Data Breach Response Team (DBRT)	Coordinate the response to significant, complex or potentially notifiable data breaches. The Data Breach Response Team will be convened where a data breach is assessed as significant, complex or likely to meet the criteria of an Eligible Data Breach. The DBRT comprises representatives from relevant business, operational and corporate functions, including TGC, IT Services and senior leadership as appropriate. The DBRT is responsible for coordinating assessment, containment, remediation and communication activities; recommending whether the breach constitutes an Eligible Data Breach; and endorsing proposed notification actions for approval through the Commission's governance arrangements.
Executive Leadership Board	Provide oversight for significant data breaches, including high-risk matters and endorsement of response and notification approaches where required.
IT Services	Lead the technical response to cyber security-related data breaches, including containment, investigation, evidence preservation, recovery activities and technical input to inform breach assessment and remediation.
Directors and Managers	Ensure effective management of data breaches within their areas of responsibility, including supporting timely reporting, escalation, and local

	management of data breaches in accordance with this Policy and the Data Breach Response Plan.
All staff	Immediately report actual, suspected or potential data breaches through established reporting channels, comply with this Policy and the Data Breach Response Plan, maintain awareness of privacy and information security obligations, and complete mandatory training requirements.

Contracted service providers and third parties who manage or hold information on behalf of the Commission must notify the Commission of any actual, suspected or potential data breach involving that information as soon as practicable and support the Commission's assessment, containment, notification and remediation activities.

5. Register of Eligible Data Breaches

The Commission maintains a register of Eligible Data Breaches in accordance with the requirements of the *Information Privacy Act 2009 (Qld)* and the Mandatory Notification of Data Breach (MNDB) scheme.

The register records relevant details of Eligible Data Breaches, including the nature and date of the breach, actions taken to contain and mitigate harm, assessment outcomes, notification decisions, and any notifications made to the Office of the Information Commissioner (OIC) and affected individuals.

The register supports the Commission's compliance obligations and ongoing monitoring, review and improvement of data breach management practices.

6. Recordkeeping

The Commission maintains appropriate records in relation to all actual, suspected and potential data breaches in accordance with the *Public Records Act 2023 (Qld)*, the *Information Privacy Act 2009 (Qld)*, and relevant recordkeeping policies and standards. Records must be accurate, complete and retained in a manner that supports accountability, legislative compliance and effective review of data breach management practices. Records include, but are not limited to, reports of suspected breaches, containment and mitigation actions, assessment activities, decision-making, reasons for applying or not applying notification exemptions, notifications made, remediation actions and post-incident review outcomes.

7. Considerations

7.1. Consideration of Human and Child Rights

The policy upholds:

- Right to privacy and reputation
- Right to equality before the law and non-discrimination
- Right to recognition and equality before the law (procedural fairness)
- Right to take part in public life (indirectly through the policy via engaging with reviews and providing submissions and evidence)
- Right to protection of families and children

7.2. Consideration of the Child Safe Standards and Universal Principle

The policy supports the Commission's commitment to safeguarding children and young people by embedding child-safe considerations into information security practices, systems and organisational culture.

The following matters have been taken into consideration in developing this policy:

1. Protection of children's personal and sensitive information
2. Risk-based approach to child safety and information security
3. Safe access to information and systems
4. Accountability, governance and oversight
5. Incident response and harm minimisation
6. Staff awareness and shared responsibility
7. Child-centred and culturally safe practices
8. Supporting participation and trust
9. Continuous improvement of child-safe capability.

This policy supports the Child Safe Standards and Universal Principle by ensuring that information security practices protect children's personal and sensitive information, promote strong governance and accountability, support safe participation, and reduce risks that could cause harm to children. Through risk-based controls, staff awareness, and effective incident management, the Commission strengthens its capacity and culture to operate as a child-safe organisation.

7.3. Consideration of Reframing the Relationship commitments

This policy supports the Queensland Government's Reframing the Relationship commitments by embedding respect, accountability and shared responsibility for Aboriginal and Torres Strait Islander peoples into information security practices, governance and organisational culture.

This policy supports Reframing the Relationship commitments by ensuring that information security practices respect Aboriginal and Torres Strait Islander peoples, protect culturally sensitive information, support transparency and shared decision-making, and strengthen trust. Through strong governance, culturally capable practices and continuous improvement, the Commission reinforces its commitment to respectful partnerships and accountable public sector leadership.

7.4. Consideration of risk management

This policy supports the Commission's risk management framework by identifying, managing and mitigating information security risks that may impact the achievement of organisational objectives, service delivery, compliance obligations and stakeholder trust.

This policy serves as a key control for mitigating information security risks identified in the Commission's Strategic and Operational Risk Registers by establishing clear requirements, responsibilities and governance arrangements for protecting information.

7.5. Consideration of privacy

This policy supports the Commission's obligations to manage personal information in a lawful, fair and responsible manner, and to protect the privacy of individuals whose information is collected, stored, used or disclosed by the Commission.

This policy supports effective privacy management by embedding information security controls that protect personal information, promote lawful and responsible information handling, and support transparency, accountability and public trust.

8. Legislative and regulatory requirements

This policy complies with the requirements of the:

- *Information Privacy Act 2009 (IP Act) (Qld)*
- *Public Records Act 2023 (Qld)*
- *Public Sector Ethics Act 1994 (Qld)*
- *Hospital and Health Boards Act 2011 (Qld)*
- *Family and Child Commission Act 2014 (Qld)*
- *Child Safe Organisations Act 2024 (CSO Act) (Qld)*
- Queensland Government Information and Cyber Security Policy (IS18:2025)
- Cybersecurity laws and regulations applicable to Queensland Government agencies.

9. Related documents

This policy should be read in conjunction with the following documents:

- Data Breach Response Plan
- Privacy Policy
- Information Security Policy
- Security Incident Reporting Policy
- Administrative Release of Information Policy
- QFCC Risk Management Framework
- Root Cause Analysis Procedure
- Recordkeeping Procedure

These documents collectively support the Commission's obligations under the *Information Privacy Act 2009 (Qld)* and the Mandatory Notification of Data Breach (MNDB) scheme and related governance requirements.

10. Definitions

In support of this Policy:

Term	Definition
Data breach	Unauthorised access to, or unauthorised disclosure of, information held by the Commission, or the loss of information in circumstances where unauthorised access or disclosure is likely to occur.
Eligible Data Breach	An Eligible Data Breach, as described in section 47 of the *Information Privacy Act 2009 (Qld)*, occurs where: • there has been unauthorised access to, or unauthorised disclosure of, personal information held by the Commission, and the access or disclosure is likely to result in serious harm to an individual to whom the information relates; or • personal information held by the Commission is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and the loss is likely to result in serious harm to an individual to whom the information relates.

Term	Definition
Unauthorised disclosure of information	The release, communication or making available of information to a person or entity who is not authorised to receive it, whether intentionally, accidentally or otherwise without lawful authority or approval.
Personal information	Personal information, as described in the *Information Privacy Act 2009 (Qld)*, means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether it is recorded in a material form or not.
Serious harm	Serious harm, as described in Schedule 5 of the *Information Privacy Act 2009 (Qld)*, refers to harm that may result from a data breach, including physical, psychological, emotional, financial or reputational harm to an individual. In assessing whether serious harm is likely to occur, the Commission may consider factors such as the sensitivity of the information, the nature of the breach, the likelihood of misuse, and the circumstances of the affected individuals.
MNDB scheme	The Mandatory Notification of Data Breach (MNDB) scheme, as established under Chapter 3A of the *Information Privacy Act 2009 (Qld)*, sets out the requirements for assessing and notifying Eligible Data Breaches.
Executive	For the purposes of this Policy, Executive refers to the Commission's senior leadership, including the Principal Commissioner, Commissioner, Chief Operating Officer and Executive Directors, as appropriate to the nature and severity of the data breach.
Affected individual	An individual whose personal information is the subject of an Eligible Data Breach.
Authorised representative	A person authorised to act on behalf of an individual, including a parent or guardian where the individual is a child.
Data Breach Response Plan	The Commission's operational document that sets out the procedures for responding to data breaches, including the response process, roles and responsibilities, and escalation pathways.
Data Breach Response Team (DBRT)	The group responsible for coordinating the management of significant, complex or potentially notifiable data breaches, including assessment, escalation, containment, remediation and notification recommendations in accordance with this Policy.

11. Document control

Document type	Policy	
Responsible Officer	Director Transformation Governance and Change	
Content Manager references	PDF version:	D26/13687
	Word version:	D26/10624
	Record of approval:	TF26/1044
Information security classification	Official This document is classified as 'Official' in accordance with the Queensland Government Information Security Classification Framework and it is suitable for public release.	

Document type	Policy
Document review	This Policy is reviewed annually, or as required following changes to relevant legislation, frameworks or organisational requirements, in accordance with the Commission's Policy Framework.

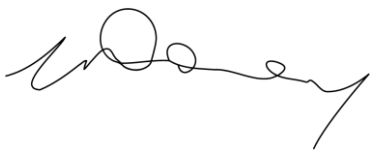
11.1 Version control

Version	Date	Description of revisions	Author
1.0	July 2026	First approved version	Manager Governance and Risk

12. Approval

This Policy is approved by the Chief Operating Officer as the accountable officer.

Signature:



Libby Doney
A/Chief Operating Officer
Queensland Family and Child Commission

Date: 5 August 2026