7.8. DATA BREACH POLICY

REPORT AUTHOR	Governance and Information Officer
EXECUTIVE	General Manager Corporate and Communities
DEPARTMENT	Corporate and Communities
TEAM	Governance
DATE	27 July 2026

RECOMMENDATION

That Council adopt the Data Breach Policy.

EXECUTIVE SUMMARY

The *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (IPOLA) introduced significant changes to the *Information Privacy Act 2009* (Qld) (IP Act), including Mandatory Notification of Data Breach (MNDB) provisions.

The MNDB provisions have been in effect for most Queensland public sector agencies since 1 July 2025, however, were deferred until 1 July 2026 for local government.

To comply with the MNDB provisions, agencies need to prepare and publish a Data Breach Policy pursuant to Section 73 of the IP Act to detail how an agency will manage and respond to data breaches. In addition, agencies must maintain a Register of Eligible Data Breaches.

PREVIOUS COUNCIL CONSIDERATIONS / RESOLUTIONS

This is a new policy and therefore there are no applicable previous considerations or resolutions.

REPORT/BACKGROUND

This Data Breach Policy has been drafted using templates and guidelines provided by the Office of the Information Commissioner (OIC).

FINANCIAL AND RESOURCE IMPLICATIONS

A serious data breach could result in significant financial and resource implications for Council.

RISK MANAGEMENT IMPLICATIONS

Failing to adopt the Data Breach Policy would result in non-compliance with Queensland legislation.

ENVIRONMENTAL IMPLICATIONS

There are no environmental implications associated with the adoption of this policy.

SOCIAL IMPLICATIONS

Data breaches can have a significant impact on the privacy of individuals in the community.

CORPORATE AND OPERATIONAL PLAN

This report has been prepared in accordance with the following:

Corporate Plan 2025-2030 Initiatives:

Theme 3 - Service Delivery
We deliver Council services effectively and efficiently to meet community expectations, focusing on the wellbeing of both the community and our employees.
3.7 - *Identify and manage risk.*

Operational Plan 2026-2027 Actions:

Legislative requirement.

LEGISLATION AND POLICY

- *Information Privacy Act 2009 (Qld).*
- *Information Privacy and Other Legislation Amendment Act 2023 (Qld).*

CONSULTATION

Internal Consultation:

- General Manager Corporate and Communities
- Council Workshop on 23 June 2026

CONCLUSION

To comply with the MNDB provisions, agencies need to prepare and publish a Data Breach Policy pursuant to Section 73 of the IP Act to detail how an agency will manage and respond to data breaches.

The recommendation for the Ordinary meeting is that Council adopt the Data Breach Policy.

ATTACHMENTS

1. Data Breach Policy [**7.8.1** - 6 pages]

98. DATA BREACH POLICY

Purpose

The purpose of this policy is to provide a framework for identifying, managing, and responding to privacy data breaches at Douglas Shire Council (Council) to ensure compliance with the *Information Privacy Act 2009* (Qld) (the IP Act).

Scope

This policy applies to all Councillors and Council employees, regardless of their employment status (full time, part time, casual, contract, or volunteer). It covers all data breaches at Council, whether accidental or intentional, and includes data contained within physical and digital records.

Policy Statement

The *Information Privacy and Other Legislation Amendment Act 2023* (Qld) introduced significant changes to the IP Act, including Mandatory Notification of Data Breach (MNDB) provisions. The MNDB provisions require agencies to take certain actions in response to Eligible Data Breaches, including assessing, containing, mitigating, and reporting breaches.

Section 73 of the IP Act also requires agencies to prepare and publish a Data Breach Policy detailing how an agency will respond to a data breach or suspected data breach. This policy aims to comply with the IP Act and MNDB provisions, protect the privacy rights of individuals, safeguard the information held by Council, and minimise the potential harm that could result from a data breach.

What Is an Eligible Data Breach?

A data breach is defined in the IP Act as an unauthorised access to, or unauthorised 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.

An Eligible Data Breach is a data breach that involves personal information. An Eligible Data Breach is defined in s 47(1) of the IP Act as an unauthorised access to, or disclosure, or loss of, personal information that is 'likely to result in serious harm' to an affected individual.

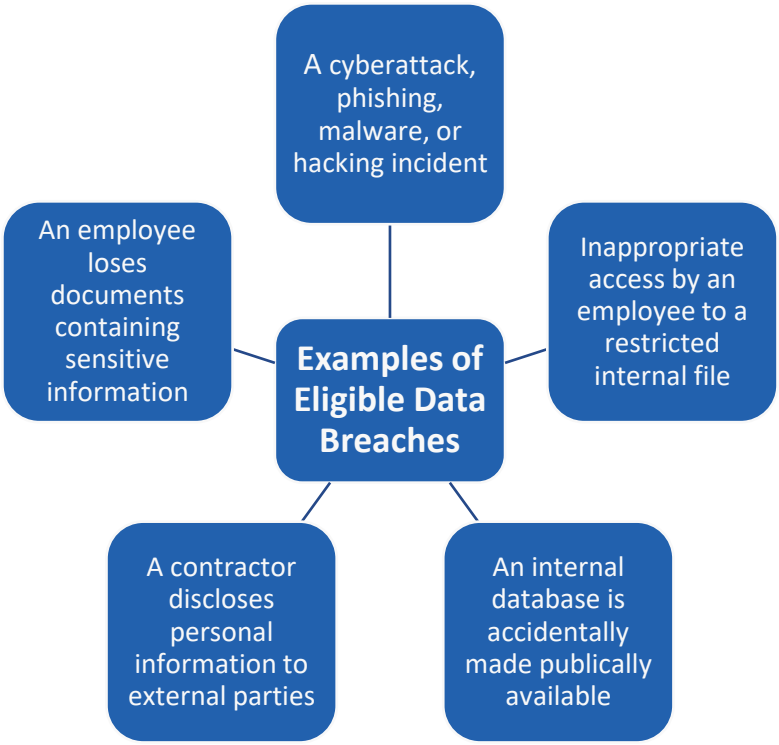
Section 47(2) of the IP Act outlines the factors to consider when assessing whether the likely harm is 'serious harm'. These factors include the kind of personal information disclosed, sensitivity of the personal information involved, and the persons who have or may have obtained the personal information subject to the breach.

Examples of Eligible Data Breaches

A data breach can happen in various ways. Examples include by malicious actions of third parties, human error, or a failure in cyber or security systems. However, not all data breaches will be Eligible Data Breaches and engage the MNDB provisions.

Where a data breach involves personal information and any impacted individuals may be seriously harmed, then the data breach will most likely be an Eligible Data Breach.

Specific Examples of Eligible Data Breaches



Roles and Responsibilities

Council Employees

Council employees must comply with the IP Act, including protecting personal information held by Council from unauthorised access, disclosure, or loss.

Council employees are required to read this Data Breach Policy and understand what is expected of them. Data breaches or suspected data breaches must be reported to an appropriate officer (this could be a Team Leader, Coordinator, Manager, or a member of the Governance Team).

Council employees must also respond to requests for information from the Governance Team and/or the Data Breach Response Team and comply with record keeping obligations.

Team Leaders, Coordinators and Managers

All employees with supervisory responsibilities must escalate concerns of data breaches or suspected data breaches within their area of responsibility to the Governance Team, General Managers or Chief Executive Officer (CEO).

Governance Team

The Manager Governance is responsible for assessing the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates.

When an Eligible Data Breach is identified, the Governance Team are to notify the Information Commissioner and any affected persons, as required under the IP Act.

This includes publishing, monitoring, and reviewing the currency of, any public notifications of a data breach published to the agency website under s 53(1)(c) of the IP Act.

The Governance Team are also responsible for maintaining the Register of Eligible Data Breaches and for reviewing and updating this policy.

Chief Executive Officer and Executive Leadership Team

For serious data breaches, the CEO and Executive Leadership Team may convene a Data Response Team and implement a Cybersecurity Management Plan, as appropriate.

Responding to a Data Breach

Council will follow a six-stage process in response to data breaches as recommended by the Office of the Information Commissioner.

Stage 1: Preparation

Council will ensure its readiness to respond to a data breach by:

- Having appropriate policies, procedures, and systems in place to identify, report and respond to data breaches.
- Clearly identifying specific reporting lines, internal decision-makers, and escalation points.
- Providing training across Council to ensure there is a broad awareness of the data breach policies, procedures, systems, and obligations.

Stage 2: Identification

Council will comply with its identification and reporting obligations by:

- Conducting an initial assessment to determine whether a data breach has occurred.
- Reporting suspected data breaches to the Office of the Information Commissioner.
- Securely documenting the details of any data breaches, including the date, time, and nature of the breach.

Stage 3: Containment and Mitigation

Council will minimise any potential harm that could result from a data breach by:

- Undertaking a preliminary risk assessment of the data breach.
- Containing the data breach and preventing further unauthorised access or disclosure.
- Implementing measures to mitigate any harm.

Stage 4: Assessment

Council will consider the scope and impact of any data breach by:

- Assessing the type of data involved and number of individuals affected.
- Determining if the data breach has the potential to cause serious harm.
- Establishing whether the breach meets the criteria for an Eligible Data Breach under the IP Act.

Stage 5: Notification

If a data breach is assessed as an Eligible Data Breach, Council will notify the Office of the Information Commissioner and affected individuals as soon as practicable. Notifications will include the information required pursuant to s 51 and s 53 of the IP Act.

When to Notify Particular Individuals

Individuals affected by a data breach will be notified as soon as practicable once sufficient information about the breach has been ascertained.

How to Notify Particular Individuals

How affected individuals affected by the data breach are notified will depend on the type and scale of the breach, as well as the immediate practical issues such as having contact details for the affected individuals.

If individuals cannot be notified directly, the required information will be published on Council's website for a period of at least 12 months, in accordance with s 53(1)(c) of the IP Act.

Stage 6: Review and Remediation

Council will conduct a post data breach review by:

- Identifying the cause of the breach and evaluating the effectiveness of the response.
- Implementing corrective actions to prevent future breaches, such as improved security measures or additional training.

Register of Eligible Data Breaches

Council will maintain a Register of Eligible Data Breaches in compliance with s 72 of the IP Act. The Register will be maintained by the Governance Team.

Record Keeping

Council will keep a record of all data breach incidents, whether Eligible Data Breaches or not, in accordance with the *Public Records Act 2002* (Qld). Records will include evidence of compliance with this policy and relevant legislation.

Definitions

TERM	DEFINITION
Affected Individual	As defined in s 47(1)(ii) of the IP Act.
Chief Executive Officer	Officer with appointment held under s 194 of the *Local Government Act 2009* (Qld). This includes any person acting in this position.
Council Employee/s	All persons employed by Council on a permanent, temporary, or casual basis, including persons engaged under a contract of service and volunteers.

TERM	DEFINITION
Councillor/s	Mayor, Deputy Mayor, and Councillors as elected representatives of Council.
Data Breach	The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
Eligible Data Breach	An Eligible Data Breach will have occurred under s 47 of the IP Act where: • There has been unauthorised access to, or unauthorised disclosure of personal information held by an agency; and • The access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or • There has been loss of personal information held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information; and • The loss is likely to result in serious harm to any of the individuals to whom the information relates.
Held or Hold	Personal information is held by a relevant agency, or the agency holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant agency.
Information Commissioner	The Queensland Information Commissioner.
Personal Information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: • Whether the information or opinion is true or not, and • Whether the information or opinion is recorded in a material form or not.
Serious Harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: • 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.

Related Legislation

- *Information Privacy Act 2009* (Qld)
- *Information Privacy and Other Legislation Amendment Act 2023* (Qld)
- *Information Privacy Regulation 2025* (Qld)
- *Public Records Act 2023* (Qld)
- *Right to Information Act 2009* (Qld)
- *Right to Information Regulation 2025* (Qld)

Related Documents

- Eligible Data Breach Register
- Information Privacy Policy
- Records Management Policy

Policy Review

This policy is to be reviewed whenever legislation changes, or every four (4) years if no changes have been required to be enacted, at the direction of the CEO.

Policy Details

Policy Name	Data Breach Policy
Policy Number	98
Policy Version	1
Document Number	
Endorsed by	Chief Executive Officer
Policy Type	Statutory
Approval Authority	Council
Date Adopted	
Time Period	4 Years
Review Date	
Policy Department	Governance
Link to Corporate Plan	Strategic Theme 3 – Service Delivery
Revoked/Superseded	Nil

This policy is to remain in force until otherwise determined by Council.