AP300 PRIVACY DATA BREACH POLICY

OVERVIEW

From 1 July 2026, Chapter 3A of the *Information Privacy Act 2009* (Qld) (IP Act) requires Council to have in place a Mandatory Notification Data Breach (MNDB) Scheme for suspected/identified Eligible Data Breaches (EDB), to ensure Council:

- takes reasonable proactive steps to identify, contain, mitigate and assess the harm of a suspected/identified EDB
- complies with notification requirements
- maintains an internal EDB register.

APPLICABILITY

This policy applies to all personal information, including employee records, collected, stored, used and disclosed by Council, its workers as defined in *HRP040 Code of Conduct* and Councillors, unless otherwise exempted by legislation. It provides a summary of Council's legislative obligations and commitments in relation to the handling of a suspected/identified EDB of personal information.

This policy should be ready in conjunction with the Related Information outlined below.

LEGISLATION

Information Privacy Act 2009 (Qld)

DEFINITIONS

Affected individual – individual to whom the personal information relates, having regard to:

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 one or more security measures; and
d) if the personal information is protected by one or more security measures – the likelihood that any of those security measures could be overcome; and
e) the persons, or 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.

Agency – a minister, department, local government or public authority, however does not include an excluded entity in accordance with section 18 of IP Act.

EDB Register – register of Council's EDBs in accordance with section 72 of the IP Act.

Data Breach – unauthorised access to, or unauthorised disclosure of, information held by Council or the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

Eligible Data Breach – occurs when the following are met:

(i) a data breach has occurred; and
(ii) the unauthorised access or disclosure of the information is likely to result in serious harm to an individual (an affected individual) to whom the personal information relates, having regard to matters stated in section 47(2) of the IP Act.

Serious harm – to an individual in relation to the unauthorised access or disclosure of an individual's personal information, for eg:

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.

PRINCIPLES

Implementation of this policy provides:

- public accountability and transparency around Council's management of personal information
- compliance with the IP Act MNDB Scheme
- consistency in Council's management of a data breach involving personal information.

POLICY

1. PROACTIVE READINESS

Council is committed to proactive readiness for a potential data breach through:

- internal training and awareness
- cyber security and incident response measures
- inclusion of data/privacy breach provisions within contracts and service arrangements, including the requirement that contracted service providers notify Council in the event of a breach
- internal policies and procedures to ensure swift and coordinated action in the event of a data breach.

2. DATA BREACH KEY STEPS

2.1 Identification and reporting

A suspected/identified Council data breach involving personal information must be immediately reported. Members of the public can report a suspected Council data breach though Council's website or contact centre.

2.2 Containment and mitigation

Council will immediately take all reasonable steps to contain and mitigate the potential harm of the data breach.

2.3 Assessment

Council will undertake a comprehensive assessment of a data breach within 30 days to determine and understand:

- what occurred
- if data compromised is personal information
- if an EDB has occurred
- whether notification is required in accordance with Chapter 3A, Part 3 of the IP Act.

If further time is needed to undertake the assessment, Council will provide written notice to the Queensland Information Commissioner in accordance with section 49 of the IP Act.

2.4 Notification

If an EDB is established, Council will notify the Queensland Information Commissioner and particular individuals of the breach in accordance with Chapter 3A, Part 3 of the IP Act.

If Council becomes aware that a suspected/identified EDB may affect another Agency, Council will provide written notice in accordance with section 48(4) of the IP Act.

2.5 Review

After a data breach has been addressed, Council will review the assessment and actions undertaken following the breach to identify and implement improvements in systems and processes.

2.6 EDB Register

Council will maintain an internal register of each EDB in accordance with section 72 of the IP Act.

3. PRIVACY COMPLAINTS

To be handled in accordance with *AP174 Privacy Policy*.

RELATED INFORMATION

Content Manager container: 109/268/189/462
Information Privacy Act 2009 (Qld)
Privacy Act 1988 (Cth)
AP174 Privacy Policy
AP298 Privacy Procedure
AP299 Privacy Guideline
AP301 Privacy Data Breach Procedure
ICT07 – Information Security Procedure
ICT30 – Acceptable Access and Use of ICT Procedure