Information Privacy Data Breach Policy

Information Privacy Act 2009

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

Contents

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

1. Policy Statement

Townsville City Council (Council) is committed to protecting the personal information it holds and to responding promptly, effectively and lawfully to data breaches.

This policy outlines Council's approach to preparing for, identifying, containing, assessing and remediating data breaches, including suspected and confirmed eligible data breaches, in accordance with the *Information Privacy Act 2009* (IP Act) and best practices.

This policy is to be read in conjunction with Council's Information Privacy Policy.

2. Principles

Council's response to data breaches is guided by the following principles:

- **Protection of individuals:** Actions will prioritise reducing the risk of serious harm to affected individuals.
- **Lawful and accountable decision-making:** Responses will comply with the IP Act and be appropriately documented.
- **Proportionality and flexibility:** Responses will be tailored to the nature, scale and risk of the incident.
- **One-Council approach:** Data breaches will be managed through a coordinated, multidisciplinary response.
- **Transparency:** Council will communicate clearly with the Office of the Information Commissioner and affected individuals where required.
- **Continuous improvement:** Council will review and improve controls, processes and training following incidents.

3. Scope

This policy applies to all Councillors, workers and third-party service providers who handle personal information on behalf of Council.

This policy applies to all personal information held by, or under the control of, Council in any form.

4. Responsibility

Role	Responsibility
Councillors, Workers and Third-Party Service Providers	Responsible for: • identifying and immediately reporting any potential, suspected or actual data breaches; • cooperating with investigations; and, • complying with record keeping obligations.
Managers	Responsible for: • ensuring that all workers understand and adhere to this

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

Role	Responsibility
	policy; • escalating incidents within their area of responsibility; and, • supporting containment and mitigation actions.
Chief Digital and Information Officer	Responsible for: • leading response to cyber security incidents; • containing and remediating technical impacts; and, • coordinating with the Governance, Risk and Compliance Team.
Digital Information and Technology	Responsible for: • establishing, implementing and maintaining Council's information security management systems, including detecting and reviewing data breaches; • managing serious or complex data breaches requiring a whole of Council response.
Legal Services (Governance, Risk and Compliance (GRC) Team)	Responsible for: • maintaining the accuracy and currency of this policy; • coordinating privacy assessment; • assessing whether a data breach is an eligible data breach; • advising on notification obligations; • coordinating information and training on information privacy data breaches; and, • maintaining the register of eligible data breaches.
Communications and Customer Experience	Responsible for managing internal and external communications relating to a data breach.
Contract Managers	Responsible for ensuring service providers comply with breach notification requirements.

5. Definitions

Term	Definition
Affected Individual	means an individual, to whom the personal information relates, who is likely to experience serious harm as a result of an eligible data breach (as per Schedule 5 and Section 47(1)(a)(ii) of the IP Act).
Councillor	means all representatives elected to the Council, including the Mayor.

Term	Definition
Data Breach	of Council, means either of the following in relation to information held by Council – (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. (as per Schedule 5 of the IP Act)
Disclosure	Council discloses personal information to another entity (the second entity) if – (a) the second entity does not know the personal information, and is not in a position to be able to find it out; and (b) Council gives the second entity the personal information, or places it in a position to be able to find it out; and (c) Council ceases to have control over the second entity in relation to who will know the personal information in the future.
Eligible Data Breach	means a data breach of Council that occurs in relation to personal information held by Council 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 to whom the personal information relates, having regard to the following: 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 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. (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

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

Term	Definition
	to result in serious harm to an individual to whom the personal information relates, having regard to the following: 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. (as per Section 47 of the IP Act)
Employees	includes any persons employed directly by Council but does not include volunteers, contractors, labour hire or contract personnel.
Manager	an individual responsible for overseeing and coordinating specific functions, departments, teams or projects within Council.
Personal Information	means information or an opinion about an 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 (as per Section 12 of the IP Act).
Sensitive Information	for an individual means: (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;

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

Term	Definition
	(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. (as per Schedule 5 of the IP Act)
Serious Harm	to an individual in relation to the unauthorised access to unauthorised disclosure of the individual's personal information, includes, for example – (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. (as per Schedule 5 of the IP Act)
Unauthorised Access	Occurs when information held by an agency is accessed by someone who is not authorised to do so.
Unauthorised Disclosure	Occurs when Council intentionally or unintentionally discloses personal information without authority.
Workers	includes employees, contractors, volunteers and all others who perform work on behalf of Council.

6. Policy

6.1. Reporting a Data Breach

6.1.1. Internal Reporting

Councillors, workers and third-party service providers must immediately report any potential, suspected or actual data breach involving personal information held by, or under the control of, Council.

Internal reports must be made to the GRC Team and Digital Information and Technology.

Third-party service providers must report data breaches in accordance with the terms of their relevant agreement with Council.

6.1.2. External Reporting

Members of the public can report a suspected data breach by contacting Council through its published contact channels.

Details of external reporting channels are maintained through Council's public-facing contact information and may change from time to time.

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

6.2. Responding to a Data Breach

Council will follow a six-stage process to respond to data breaches:

6.2.1. Preparation

Council will maintain readiness to prevent and respond to data breaches through:

- an up-to-date data breach response plan and supporting incident response arrangements;
- regular training and awareness activities for Councillors and workers; and
- information security and access controls proportionate to the risks associated with Council's information holdings.

6.2.2. Identification

Council will ensure suspected data breaches are promptly recorded and triaged to confirm whether a data breach has occurred and whether personal information may be involved.

Council will document the key details of the incident, including (where known) the date, time, nature and circumstances of the suspected breach.

6.2.3. Containment and Mitigation

Council will take immediate and reasonable steps to contain and mitigate a data breach as soon as possible after the breach is identified, to prevent further unauthorised access, unauthorised disclosure or loss and to reduce the risk of serious harm to affected individuals.

Containment and mitigation actions will be proportionate to the nature and risk of the incident and will be documented.

6.2.4. Assessment

Where Council knows or reasonably suspects that a data breach may be an eligible data breach, Council will assess whether there are reasonable grounds to believe an eligible data breach has occurred.

In conducting the assessment, Council will consider, as a minimum:

- the type and sensitivity of the personal information involved;
- the circumstances of the unauthorised access, unauthorised disclosure or loss;
- the number of individuals (or classes of individuals) likely to be affected;
- whether the breach is likely to result in serious harm to any affected individual; and
- any containment or mitigation actions already taken and their effectiveness.

The assessment will be completed within 30 days of forming the suspicion, unless an extension is required under the IP Act. Where an extension is required, Council will notify the Information Commissioner within the initial 30-day period.

6.2.5. Notification

If Council reasonably believes an eligible data breach has occurred, Council will, as soon as practicable:

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

- provide a written statement to the Information Commissioner in accordance with sections 51 and 52 of the IP Act; and
- notify affected individuals in accordance with section 53 of the IP Act, unless an exemption applies.

Notification must be clear, accurate, and include, as a minimum:

- a description of the eligible data breach;
- the type of personal information involved;
- recommended steps affected individuals can take to reduce the risk of serious harm; and
- contact details for further information.

Where notification is not required (including where Council relies on an exemption), Council will document the reasons for that decision.

Depending on the circumstances, Council may also be required to notify or engage with external parties such as insurers, law enforcement, regulators or other agencies.

6.2.6. Post Data Breach Review and Remediation

Following management of a data breach, Council will conduct a post-incident review to:

- identify the root cause of the data breach and any systemic, control, or process weaknesses;
- evaluate the effectiveness of Council's response (including containment, assessment and notification actions, where applicable); and
- implement remediation and corrective actions to prevent recurrence, including improvements to policies, controls, processes, and training.

6.3. Register of Eligible Data Breaches and Recordkeeping

Council will maintain an internal register of eligible data breaches in accordance with section 72 of the IP Act.

The Register will include, as a minimum:

- details of the breach (including the date, nature and scope of the breach);
- actions taken to contain and mitigate the breach;
- assessment outcomes and decisions relating to notification (including any reliance on an exemption); and
- post-incident review findings and remediation actions.

Council will ensure that all data breach incidents, whether eligible or not, are documented and retained in accordance with the *Public Records Act 2023*.

6.4. Complaint Management

Privacy complaints will be managed in accordance with Council's Information Privacy Policy.

7. Legal Parameters

Human Rights Act 2019

Information Privacy Act 2009

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026

Information Privacy Regulation 2025
Local Government Act 2009
Local Government Regulation 2012
Public Records Act 2023
Right to Information Act 2009

8. Associated Documents

Business Continuity Management Policy

Information Management Policy

Information Privacy Policy

ISO 27001 Information technology - Security techniques - Information security management systems

Queensland Government Information and Cyber Security Policy (IS18)

Records Governance Policy

Document Set ID: 28502749
Version: 2, Version Date: 17/06/2026