DATA BREACH POLICY

Dungog Shire Council

2023

Table of Contents

1 BACKGROUND

Changes to the Privacy and Personal Information Protection Act (PPIP Act) and the introduction of the Mandatory Notification of Data Breaches Scheme represent a significant change to how Council promotes, supports, and practises responsible privacy governance.

Under part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act), Council is required to notify the Privacy Commissioner (and affected individuals) of eligible data breaches.

Council is also required to prepare and publish a Data Breach Policy (this Policy) in accordance with section 59ZD of the PPIP Act to manage such breaches.

2 PURPOSE

The purpose of this Policy is to outline how data breaches are managed at Council, and the roles and responsibilities of staff involved.

3 SCOPE

This Policy applies to all Council staff, Councillors, contractors, volunteers and authorised users of Council's information and communication technologies.

This Policy applies to eligible data breaches as defined in this Policy and does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual.

Where breaches are not covered by this Policy, Council is not required to notify individuals or the Commissioner but will still take appropriate action to respond to the breach. Council may still provide voluntary notification to individuals where appropriate.

4 PRINCIPLES

Dungog Shire Council is committed to:

- Ensuring personal information is protected in accordance with Council's Privacy Management Plan and relevant legislation
- Ensuring instances of data breaches are responded to quickly.

5 DEFINITIONS

Eligible data breach	An 'eligible data breach' occurs where: 1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector

	agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and 2. A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates. Breaches can occur between agencies, within an agency and external to an agency.
Personal information	As defined in section 4 of the Privacy and Personal Information Protection Act 1998, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

6 ROLES AND RESPONSIBILITIES

General Manager

The General Manager is responsible for:

- Ensuring that Council is compliant with relevant legislation surrounding data breaches
- Determining whether to undertake external notification when a data breach occurs
- Undertaking external notifications to affected individuals/ organisations and the NSW Privacy Commissioner
- Notifying Council's insurers as required.

Cyber Response Team

The Cyber Response Team will be led by the Executive Manager Corporate and Customer Service (or delegate), and will include the Information Systems Administrator, and other relevant staff, as appropriate.

The Cyber Response Team is responsible for:

- Communicating to staff about cyber safety and encouraging the reporting of suspected data breaches and cyber security events
- Maintaining and reviewing this Policy
- Maintaining an internal register of eligible data breaches
- Maintaining and publishing a public notification register on Council's website for any notifications made under section 59N(2) of the PPIP Act.
- Conducting a post-breach review and providing an evaluation report to Council's Executive Leadership Team for information.
- Determining reporting obligations including notification to the IPC, affected individuals, external stakeholders or other bodies.

All Employees

All employees are responsible for immediately reporting any actual or suspected data breaches to Council's Information Systems Administrator.

7 PREPARING FOR A DATA BREACH

In order to ensure Council is prepared in the event that a data breach occurs, Council will provide training to employees on the importance of safeguarding personal information and how to identify and report a potential data breach.

8 RESPONDING TO A DATA BREACH

When a data breach is reported, it is imperative that Council responds quickly to minimise the loss of personal information.

8.1 Containing a data breach

When a data breach has occurred, an initial assessment will be conducted by the Cyber Response Team (see Roles and Responsibilities for further information).

The Cyber Response Team will act to contain a data breach or suspected data breach to minimise the possible damage.

8.2 Assessing a data breach

Once the data breach has been contained, the Cyber Response Team will compile a report on the data breach and assess/evaluate the information involved in the breach. A risk assessment will also be conducted in accordance with Council's Risk Management Framework.

The report and risk assessment will be used to determine the next steps and any additional actions identified to mitigate risks.

8.3 Managing a data breach

The Cyber Response Team will escalate to the General Manager when a data breach has occurred and external notification to affected individuals or the Privacy Commissioner is required.

9 RECORD KEEPING

Council will maintain appropriate records to provide evidence of how suspected breaches are managed, including those not escalated to the response team or notified to the Privacy Commissioner. Records will be managed in accordance with Council's Records Management Policy.

Recording data breaches allows organisations to monitor, analyse and review the type and severity of suspected breaches along with the effectiveness of the response methods. This may help agencies to identify and remedy weaknesses in security or processes that are prone to error.

10 POST-BREACH REVIEW AND EVALUATION

Following a data breach, Council will conduct a review of relevant controls, systems and processes that may have contributed to the data breach. This will form part of the post-breach evaluation, which will identify actions Council will take in response to the data breach to strengthen Council's cyber security and further prevent future data breaches occurring.

11 POLICY ADMINISTRATION

Responsible Officer:	Information Systems Administrator
Council or Management:	Council
Adoption date:	20/09/2023
Next review date:	20/09/2027
TRIM ID:	23/25249
Version history	N/A
Relevant legislation:	Privacy and Personal Information Protection Act 1998 (NSW) ss. Part 6A, 59D, 59N(2), 59ZD Privacy and Personal Information Protection Amendment Bill 2021 Health Records and Information Privacy Act 2002 State Records Act 1998 (NSW) Government Information Classification and Labelling Guidelines 2013 (NSW)

CONTACT US

198 Dowling Street,
Dungog NSW 2420
shirecouncil@dungog.nsw.gov.au
02 4995 7777