BYRON SHIRE COUNCIL

DRAFT Policy

Data Breach

2023

Information about this document

Date Adopted by Council	
Resolution No	
Document Owner	Director Corporate and Community Services
Document Development Officer	Manager Business Systems and Technology
Review Timeframe	4 years
Last Review Date	15 November 2023
Next Scheduled Review Date	15 December 2027

Document History

Doc No.	Date Amended	Details/Comments e.g. Resolution No.
E2023/108480	19/10/2023	First draft

Further Document Information and Relationships

Related Legislation	• Local Government Act 1993 (NSW) • Local Government (General) Regulation 2021 (NSW) • Privacy and Personal Information Protection Act 1998 (NSW); • Privacy Act 1988 (Cth) (for Tax File Numbers); • Health Records and Information Privacy Act 2002 (NSW); • Government Information (Public Access) Act 2009 (NSW) • Data Sharing (Government Sector) Act 2015 (NSW) • Workplace Surveillance Act 2005 (NSW)
Related Policies	• Risk Management Policy
Related Standards, Procedures, Statements, documents	• Privacy Management Plan • Cyber Security Incident Response Plan • Risk Management Strategy • Code of Conduct • Business Continuity Plan and Sub-plans • Disaster Recovery Plans

CONTENTS

1. Introduction

1.1 Objectives

The Data Breach Policy sets out how Council will respond to unauthorised access, or a loss of information held by Council. The policy details:

- what constitutes an eligible data breach under the *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps involved in responding to a data breach and reviewing systems, policies, and procedures to prevent future data breaches.

1.2 Scope

This policy applies to all staff and contractors of Council. This includes temporary and casual staff, private contractors and consultants engaged by Council. This policy also applies to third party providers, who hold personal and health information on behalf of Council.

1.3 Definitions

Listed here are all the terms and acronyms used in the Policy, and their definitions.

Policy acronym	**Definition**
Affected Individual	means an “affected individual” as defined in the PPIP Act.
Council Held Information	means any personal information in whatever form (including hard copy, and electronically held information), which is held by Council or is otherwise in the possession or control of Council.
Council Officer	means any officer or employee of Council.
Data Breach	means the unauthorised access to, or inadvertent disclosure, access, modification, misuse, or loss of, or interference with personal information, and in this Policy includes a potential data breach.
Eligible Data Breach	means an “eligible data breach” as defined in s59D of the PPIP Act.
HRIP Act	means the Health Records Information and Privacy Act 2002 (NSW).
IPC	means the Information and Privacy Commission of NSW.
IT	means information technology.

Mandatory Reporting Data Breach	means notification for an eligible data breach as defined in the PPIP Act.
Personal Information	means any information defined as “personal information” under the Privacy Act, PPIP Act, or “health information” under the HRIP Act.
PPIP Act	means the Privacy and Personal Information Protection Act 1988 (NSW).
Privacy Act	means the Privacy Act 1988 (Cth).

2. Statement

A data breach occurs when there is an incident that has caused or has the potential to cause unauthorised access to or disclosure or loss of Council held information. Examples include:

- accidental loss or theft of Council held information or equipment on which such Council Information is stored;
- unauthorised use, access to or modification of Council held information or information systems;
- unauthorised disclosure of classified Council held information, or Council information posted onto the website without consent;
- a compromised Council officer’s user account;
- successful attempt to gain unauthorised access to Council’s information or information systems;
- equipment failure;
- malicious disruption to or denial of IT services.

A Data Breach may occur directly from the Council or from a contractor or business partner of the Council who has custody of, or access to, Council held information.

2.1 When does Council report a data breach?

Mandatory reporting of a data breach as defined in the PPIP Act generally applies where there is unauthorised disclosure or access to personal information **and** it is reasonably considered that there could be serious harm to individuals to whom the information relates. This is known as an eligible data breach.

Determining whether a data breach is subject to mandatory reporting obligations requires a specific assessment by senior Council officers, and may also be determined based on legal advice.

Reporting is made to the Information and Privacy Commission (IPC) and any affected third parties.

3. Legislative and strategic context

Council has obligations under the PPIP Act, the HRIP Act and the Privacy Act including mandatory reporting obligations in respect of data breaches. This policy only relates to data breaches. Council's Privacy Management Plan provides more information on how Council may collect, use and disclose personal information.

4. Governance

Council maintains an effective and integrated risk management framework, allocating resources, responsibility, and accountability to manage risks across the organisation. Refer to Council's Enterprise Risk Management Policy for further information.

4.1 IT controls

In addition, Council has a comprehensive set of information technology controls. This includes robust access controls, data encryption, patch management, network and endpoint security measures, and incident response plans to ensure all IT assets are properly secured and monitored. Regular penetration testing and vulnerability scanning are performed to identify and remediate any weaknesses identified in the IT systems.

4.2 Training and awareness

To mitigate the risk of data breaches Council has established a comprehensive training program to educate employees about the risks associated with data breaches and their responsibilities in recognising, responding, reporting and preventing such incidents. Council conducts regular phishing simulation exercises to assess employee readiness for data breach incidents and to raise awareness of the dangers of phishing and social engineering.

4.3 Contractors and third parties

Council will require all contracts with contractors who may be provided with, have access to or hold Council held information, to contain obligations requiring the contractor to report data breaches to Council, take mitigating actions and assist Council in undertaking assessments of the data breach. Contractors will also identify who will notify any affected individuals and provide support in the event of a data breach. For data breaches that involve other public agencies, the General Manager (or delegate) will directly liaise with other affected agencies in respect of any notification requirements for mandatory reporting data breaches.

5. Responding to a data breach

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harm to individuals and entities. There is no single way of responding to a data breach but the steps in responding include:

1. **Contain**: Minimise the data breach to prevent any further compromise of personal information.

2. **Assess**: Gather the facts, evaluate the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

3. **Notification**: Inform individuals and the IPC if required. The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations. A notification register will be available on Council's website, listing all eligible data breaches recorded in the last 12 months.

4. **Review**: Assess the incident and consider what actions can be taken to prevent future breaches. This may include a review of systems, policies, and procedures.

5.1 Council officer reporting responsibilities

Any Council officer who becomes aware of a data breach will immediately notify the relevant manager or director. Where a Council officer and/or a relevant manager or director believes, or has reasonable grounds to believe, that the data breach is a mandatory reporting data breach, the relevant manager or director will notify the General Manager (or delegate) immediately.

When reporting a possible mandatory reporting data breach to the General Manager (or delegate), a Council officer and/or a relevant manager or director will also indicate whether in their opinion it is likely to take more than 30 days to determine if the data breach is a mandatory reporting data breach (if known).

For non-eligible data breaches, a relevant manager or director will notify the Manager Corporate Services within 24 hours.

The Manager Corporate Services, on being notified of a data breach will contact the Council's insurer.

Council's Cyber Security Incident Response Plan details common incident scenarios and procedures for how to respond and report on a data breach incident.