ICT-CP-01

Data Breach Policy

1. Introduction

This policy is to provide guidance to Yass Valley Council (Council) employees, contractors, volunteers in responding to a breach of the Council held information.

2. Policy Objectives

Main objectives of this policy are to achieve an effective privacy and data breach management plan, and to create processes and procedures to comply with the Privacy and Personal Information Protection Act 1998 (PPIP Act).

3. Policy Scope

This policy applies to all Council employees, contractors, volunteers and public whose information is held by Council.

4. Policy Provisions

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to Council's held data.

Council will create and implement all necessary procedures, in order to implement the following 4 key steps in response to a data breach as per the Information and Privacy Commissioner's guidelines. The first three steps may be undertaken concurrently.

4.1 Contain the breach

Containing the breach is prioritised by the Council. Council will prepare plans and procedures, in order to take necessary steps to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords.

4.2 Evaluate the associated risks

Council will make necessary arrangements supported by an operational procedure under this policy, in order to assess the type of data involved in the breach and the risks associated with the breach. These assessments must include factors like who is affected, what data is breached and what is the foreseeable harm etc.

4.3 Notifying affected individuals

Council will develop a Mandatory Notification of Data Breach (MNDB) Scheme which will assist notifying all the individuals affected by a data breach, the NSW Information and Privacy commissioner as well as other relevant government agencies as required by relevant legislations.

4.4 Prevent a repeat

Council will make arrangements for short or long-term measures to prevent any reoccurrences. Preventative actions could include a:

a. security audit of both physical and technical security controls
b. review of policies and procedures
c. review of employees, contractors and volunteers training practices; or
d. review of contractual obligations with contracted service providers.

5. Review

This policy will be reviewed every two (2) years or as required as best practice, legislation or government polices change. Records are to be managed as per Council's records procedures.

6. Legislative and Legal Framework

This policy is to be read in conjunction with the following:

Legislation	• Privacy and Personal Information Protection Act 1998 • Health Records and Information Privacy Act 2002 • State Records Act 1998 • Local Government Act 1993
Policies and procedures	• IPC Data Breach Guidance for NSW Agencies (September 2020) • IPC Voluntary Data Breach Notification (Aug 2020) • Information and Privacy Commission Data Breach Policy (June 2020) • Sensitive and Security Classified Information Schema • Council's Privacy Management Plan

7. Definitions

Term	Meaning
Data Breach	Data breach occurs when there is a failure that has caused unauthorised access to, or disclosure of, Confidential Information held by Yass Valley Council.
Confidential Information	Information and data (including metadata) including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of significant buildings, Security Classified Information and information related to the Council's IT/cyber security systems.
Council Employee	Includes full time, part time, casual, temporary, volunteer and fixed term employees.
Health Information	A specific type of Personal Information which may include information about a person's physical or mental health or their disability, for example, medical certificates.

Personal Information	It has same definition as defined in section of PPIP Act. Examples are name, address, email address, phone number, date of birth or photographs.
Security Classified Information	Information and data (including metadata) that is marked as Protected, Secret, or Top Secret as per the Commonwealth Attorney Generals' Department's Protective Security Policy Framework.

8. Responsibilities

a. Internal notifications

The following roles will be notified of any data breach:

- Chief Executive Officer
- Director Corporate and Community
- Relevant Business Unit Director
- Relevant Business Unit Manager

b. Other Responsibilities

Director Corporate and Community Services will:

- Provide all necessary administrative support for the operation of this policy
- Develop and document any procedures for the effective implementation of this policy
- Keep sufficient records to enable monitoring of compliance with this policy and provide information required for Integrated Planning and Reporting purposes and internal organisational performance measurement.

All employees will:

- Immediately report any actual or suspected Data Breaches to the Manager ICT and or Director Corporate and Community and or CEO.

The ICT Manager will:

- Immediately notify the Data Breach Review Team and assemble the Team as soon as possible
- Undertake relevant internal notifications as required by this policy.

The Data Breach Review Team will:

- Assemble promptly to review and respond to a data breach
- Follow this policy when responding to a data breach
- Consult with internal and external stakeholders as required
- Prepare a data breach review report for each separate Data Breach incident.

The Data Breach Review Team will consist of:

- ICT Manager
- Network and Systems Administrator
- Manager Governance & Risk
- Governance Officer
- Risk Officer

The Network and Systems Administrator will:

- Take immediate and any longer-term steps to contain and respond to security threats to the Council's IT Systems and Infrastructure.

The Manager Risk and Governance will:

- Undertake notifications as required to affected individuals/organisations and the NSW Privacy Commissioner
- Notify the Council's insurers as required

c. Data breach documentation

Documentation relating to data breaches will be stored in the MagiQ document management system.

9. Approval History

10. Date	Stage	Report to	Action	Reference
28 Nov 2023	Draft	EMT	Approved	
20 Dec 2023	Original	Council	Adopted	273/23
	Review			

11. Ownership and Approval

Responsibility	Role
Author	Governance Officer & Manager ICT
Owner	Manager ICT
Endorser	Executive Management Team
Approver	Council