Council Policy

Policy Title:	**Data Breach**
Policy Number:	CPOL 8.13
Focus Area:	Provide Great Service
Responsibility:	Information and Technology Services
Meeting Adopted:	18 February 2025 [Resolution 180225/13]

OBJECTIVE

The objective of this policy is to set out how Council will respond to unauthorised access, or a loss of information held by Council. The policy details:

1. What constitutes an eligible data breach under the *Privacy and Personal Information Protection Act 1998* (PPIP Act);
2. Council's departmental roles and responsibilities for reporting, reviewing and managing data breaches;
3. The steps involved in Council responding to a data breach; and
4. Council's procedures in reviewing the systems and policies in place to prevent future data breaches.

SCOPE

This policy applies to all staff and contractors of Council, including but not limited to full and part-time permanent staff, 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.

DEFINITIONS

Policy Term or Acronym	Definition
Affected Individual	An "affected individual" as defined in s59D of the PPIP Act.
Council Held Information	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	Any officer or employee of Council.
Data Breach	The unauthorised access to, or inadvertent disclosure, access, modification, misuse, loss of, or interference with personal information, and in this Policy includes a potential data breach.
Substantial Detrimental Effect	A consequence to an affected individual that is more than mere irritation, inconvenience or annoyance.

Eligible Data Breach	An "eligible data breach" as defined in s59D of the PPIP Act: (1)(a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and 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, or (1)(b) personal information held by a public sector agency is lost in circumstances where— • unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and • if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.
HRIP Act	*Health Records Information and Privacy Act 2002* (NSW)
IPC	Information and Privacy Commission NSW
IT	Information Technology
Mandatory Reporting Data Breach	Notification of an eligible data breach as defined in the PPIP Act.
Personal Information	Any information defined as "personal information" under the Privacy Act, PPIP Act, or "health information" under the HRIP Act.
PPIP Act	*Privacy and Personal Information Protection Act 1988* (NSW)
Privacy Act	*Privacy Act 1988* (Cth)
Public Notification	A notification on Council's website made in accordance with s59N(2) of the PPIP Act, when any affected person is unable to be contacted directly by Council in the event of an eligible data breach.
Serious Harm	Injury which is the result of a data breach that has caused substantial detrimental effect to the affected individual.

POLICY

1. Legislative obligations

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

2. What is a data breach?

A data breach occurs when there is an incident that has caused or has the potential to cause an unauthorised access to, disclosure of, or loss of Council held information. Examples include but are not limited to:

- 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 Council information posted onto the website without consent;
- A compromised Council officer's user account;
- A 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. A data breach may also occur via external party infiltration (hacking).

3. When does Council report a data breach?

Section 59M of the PPIP Act prescribes a mandatory obligation on a public sector agency to report an eligible data breach. Mandatory reporting of an eligible 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.

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

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.

4. Risk Management Framework

Council maintains an effective integrated risk management framework, allocating resources, responsibility and accountability to manage risks across the organisation. Further information may be obtained by reference to Council's Risk Management Policy.

With respect to personal information, Council employs various methods to proactively protect personal information, including the following:

4.1 IT controls

Council has a comprehensive set of information technology controls to ensure all IT assets are properly secured and monitored. This includes but is not limited to:

- Robust access controls;
- Data encryption;
- Patch management;
- Network and endpoint security measures;
- Regular and ongoing systems reviews; and
- Incident response plans.

Additionally, regular penetration testing and vulnerability scanning are performed to recognise and remediate any weaknesses discovered 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 holds an extensive program of internal operational policies to engage and educate employees on expected conduct with respect to information held by Council, including:

- Cyber Crime and Security Incident
- Cloud Services
- Information Management
- Access Control
- Acceptable Use
- Personnel Management
- Remote Access
- Physical Access
- Online Services
- Legal Compliance
- Internet
- Hardware Management
- Encryption.

Additionally, Council provides ongoing advice and instruction to its employees with respect to updating of internet capable devices to ensure the latest protection is in place.

Council's IT department continue to expand their knowledge in order to remain up-to-date with current issues with respect to information management.

4.3 Contractors and third parties

Council shall 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 assessment 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. Reporting a data breach

5.1 Members of the public

If a data breach has occurred, or is suspected to have occurred, members of the public can report the breach as soon as possible by calling Council on (02) 6660 0300. Calls made outside operating hours will be responded to by an after-hours service.

Council also provides a 'Contact Council' option on the website at: richmondvalley.nsw.gov.au.

5.2 Council officers

Any Council officer who becomes aware of a data breach or possible 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 Manager Information and Technology Services, and 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 relevant manager or director will also indicate either in their opinion if 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 Information and Technology Services within 24 hours.

For eligible data breaches the General Manager (or delegate) shall proceed with mandatory notification requirements.

Council's Director Organisational Services, on being notified of a data breach, will contact the Council's insurer.

Detailed procedural actions and examples of common incident scenarios with respect to data breach are held in Council's internal operations Data Breach Response Plan.

6. Responding to a data breach

Council recognises that data breaches can be caused or exacerbated by a variety of factors, may involve different types of personal information, and give rise to a range of actual or potential harm to individuals and entities. Council also recognises that responding to a data breach will depend on the circumstances surrounding the breach, however, as a general guideline, the following steps are a minimal procedural course of action:

Procedural steps in the event of a data breach	
1. Identify	Take necessary steps to identify the data breach facts, including parties involved, particulars of the breach and any person or organisation that may be directly or inadvertently affected by the breach.
2. Contain	Minimise the data breach as far as possible to prevent any further compromise of personal information.
3. Assess	Consider the facts, evaluate the risk of harm to potentially affected parties, and formulate an action plan to mitigate the risk of harm or to remediate any harm done.
4. Notification	Inform individuals and the IPC if required. The method of notifying affected individuals/organisations will depend for the most part on the type and scale of the breach, as well as immediately practical details such as having contact details for the affected individual/organisation. If an affected person is unable to be contacted directly, a notice in accordance with ss59N(2), 59O and 59P of the PPIP Act shall be published on Council's website. This notification register will be available on Council's website listing all s59N(2) eligible data breaches recorded in the last 12 months.
5. 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, followed by necessary actions to implement review recommendations.

7. Record keeping

Council will maintain the following record keeping measures:

- An internal register of all eligible data breaches.
- A public notification register of s59N(2) notices, available on Council's website.

8. References

Health Records Information and Privacy Act 2002 (NSW)

Privacy and Personal Information Protection Act 1988 (NSW)

Privacy Act 1988 (Cth)

REVIEW

This policy will be reviewed by Council at the time of any relevant legislative changes, compliance requirements or at least every four years.

Version Number	Date	Comments
1	18 February 2025	New policy