Shoalhaven City Council

1300 293 111 | shoalhaven.nsw.gov.au

Data Breach Policy

Adoption Date:	30/10/2023
Amendment Date:	
Minute Number:	MIN23.638
Review Date:	30/10/2026
Directorate:	City Performance
Record Number:	POL23/19

Contents

1. Purpose

Shoalhaven City Council is required under s59ZD of the Privacy and Personal Information Protection Act (PPIPA) to prepare a Data Breach Policy.

Shoalhaven City Council maintains personal information such as ratepayer, resident and customer data/information from parties who interact with Council.

Council also maintains personal and workforce data/information.

This data is collected by Council as is used to plan, monitor and manage the workforce, services and properties across the Local Government Area (LGA).

Given the personal information is retained by Council to carry out its services, it is bound by the PIPPA Act and must take necessary care to manage personal data. Council must also comply with the notification requirements at s59 of the Act in the event of any data breach defined as eligible by the PIPPA Act.

This policy supplements and should be read in conjunction with Shoalhaven City Council's Privacy Management Plan.

2. Statement

The publicly accessible Policy establishes the roles and responsibilities of staff in relation to managing a breach, and the steps Council will follow when a breach occurs.

3. Provisions

3.1. How we have prepared for a data breach

Council have prepared themselves for a data breach through the Cyber Incident Response Plan as well as this policy which outlines the key controls, systems and processes used to monitor for and identify actual or suspected data breaches. Council makes use of advanced threat protection systems to prevent, detect and respond to security threats to devices and endpoints.

3.2. Record keeping requirements

Council maintains the recording of data breaches to monitor, analyse and review the type and severity of suspected breaches along with the effectiveness of the response methods. Council utilises the gathering of the relevant information through the data breach incident report. The reports and data around suspected or escalated breaches are recorded in the Information Technology Service Management system. This system is restricted to only approved users and includes all data to monitor for any repeat weaknesses in security or processes.

3.3. What is a data breach?

A data breach is an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen, or used by unauthorised individuals, whether accidentally or intentionally. Examples of data breaches include;

• a device with a customer's personal information is lost or stolen

• a database with personal information is hacked
• personal information is mistakenly given to the wrong person

The PIPPA Act specifically describes an eligible data breach at s59D(1) as follows:

(1) For the purposes of this Part, an eligible data breach means—

(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
(b) personal information held by a public sector agency is lost in circumstances where—
(i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and
(ii) 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.
(2) An individual specified in subsection (1)(a) or (1)(b)(ii) is an affected individual.

(3) To avoid doubt, an eligible data breach may include the following—

(a) a data breach that occurs within a public sector agency,
(b) a data breach that occurs between public sector agencies,
(c) a data breach that occurs by an external person or entity accessing data held by a public sector agency without authorisation.

3.4. When do we know a data breach has occurred?

Council may be made aware of a data breach through a report from a member of staff, a contractor, an affected third party or through a report from another government agency. Council may also receive a written request seeking an internal review of a privacy complaint relating to a data breach incident.

3.5. How to report a data breach

In the event of a known or suspected data breach this should be reported either verbally or in writing via the Data Breach Incident Report form to Council's CEO (or delegate) as soon as practicable who will commence the response process.

Shoalhaven City Council's CEO (or delegate) may also direct other staff under S59G of the PIPPA Act to carry out assessments of potential data breaches and whether the data breach is considered an eligible data breach.

3.6. Data Breach Response Process

3.6.1. Contain

- As soon as practicable after a potential breach is reported via the Data Breach Incident Report form to the CEO (or delegate) or the staff directed to undertake the assessment should gather the necessary information and complete the Data Breach Incident and Response Report and retain any evidence of the breach occurring.
- Necessary steps should be taken by the CEO (or delegate) or the staff directed to undertake the assessment immediately to contain the breach once details of the

incident have been gathered (this may involve coordinating with other members of staff to ensure necessary steps/measures are put in place)

- Once a preliminary assessment of the level of harm posed by the breach (high, medium, low) has been established notify the relevant stakeholders.

3.6.2. Assess

- The Response Team should review the preliminary assessment carried out by the Governance Coordinator and complete the Data Breach Incident and Response Report.
- Particular attention should be paid to the following as this will determine the implications on Council in regard to the notification process.
    - Whether the breach is likely to result in serious harm to any affected parties
- Council may engage 3rd party assistance *such as* ID Support NSW to provide support to Council and Community and / or seek advice from the NSW Information and Privacy Commission, an opinion or validate the assessment made by the Response Team.
- Any further remedial actions identified by the Response Team to contain or minimise the severity of the breach should be taken.
- Assessment of the breach should be completed as soon as practicable and at latest within 30 days of the breach being reported.

3.6.3. Notify

- As soon as possible after it has been determined that an eligible data breach has occurred S59M of the PIPPA Act requires that the CEO (or delegate) must, in the approved form, immediately notify the Privacy Commissioner of the eligible data breach. An approved form for reporting of eligible data breaches will be issued by the Privacy Commissioner.
- Individuals affected by the data breach must also be notified, where practical, as required by S59N of the PIPPA Act.
- The following information is required in notices issued to individuals under S59N of the PIPPA Act:

    (a) the date the breach occurred,

    (b) a description of the breach,

    (c) how the breach occurred,

    (d) the type of breach that occurred, Examples of a type of eligible data breach— 1 unauthorised disclosure 2 unauthorised access 3 loss of information

    (e) the personal information that was the subject of the breach,

    (f) the amount of time the personal information was disclosed for,

    (g) actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual,

    (h) recommendations about the steps the individual should take in response to the eligible data breach,

    (i) information about -

        (i) the making of privacy related complaints under Part 4, Division 3, and

(ii) internal reviews of certain conduct of public sector agencies under Part 5,

(j) the name of the public sector agency the subject of the breach,

(k) if more than 1 public sector agency was the subject of the breach—the name of each other agency,

(l) contact details for -

(i) the agency the subject of the breach, or

(ii) a person nominated by the agency for the individual to contact about the breach.

- Where Council is unable to notify all impacted individuals, or the CEO (or delegate) determines it to be appropriate public notification should be made of the breach as per s59P of the PIPPA Act. The information in the public notification must:

(a) be published on the public notification register for at least 12 months after the date the notification is published, and

(b) include the information specified in section 59O, except to the extent the information -

(i) contains personal information, or

(ii) would prejudice the agency's functions.

3.7. Post-Breach Review and Evaluation

Council will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence. Preventative actions could include a:

- Security audit of both physical and technical security controls
- Review of policies and procedures
- Review of staff/contractor training practices
- Review of contractual obligations with contracted service providers.

4. Implementation

This Policy should be read in conjunction with Council's Privacy Management Plan and Council's Cyber Security Policy.

The Core Data Breach Response Team is made up of:

- Business Assurance and Risk Manager
- Governance Coordinator
- Chief Information Officer
- Cyber Security Analyst
- IT Infrastructure and Service Delivery Manager

Depending on the nature and circumstances of the breach, other employees may be called on to form part of the data breach review team.

Responsibilities
All employees will:

- Immediately report any actual or suspected Data Breaches to the Chief Information Officer.

The Chief Information Officer 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 Core 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 Cyber Security Analyst and IT Infrastructure and Service Delivery Manager will:

- Take immediate and any longer term steps to contain and respond to security threats to the City's IT systems and infrastructure.

The Manager Business Assurance and Risk and/or Governance Coordinator will:

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

5. Review

This Policy will be reviewed every 3 years in line with Council's Privacy Management Plan.

6. Appendices

Data Breach Incident Report

<table>
<tr><td>Name/Position:</td><td>Date</td></tr>
<tr><td colspan="2">When, where and how did the breach occur?</td></tr>
<tr><td colspan="2">Who and how was the breach discovered?</td></tr>
<tr><td colspan="2">When was the breach first reported to the CEO / Governance Coordinator / Chief Information Officer?</td></tr>
<tr><td>How would you classify the breach?

○ Unauthorised Access
○ Unauthorised Disclosure
○ Loss
○ Alteration
○ Destruction of Personal Information</td><td>What information/data has been compromised?

○ Financial details
○ Tax File Number
○ Identity Information
○ Contact Information
○ Health Information
○ Other</td></tr>
</table>

What parties have been affected by the breach?
Steps taken to immediately contain the breach?
Do any external parties need to be notified about the breach? E.g. The OAIC, NSW Information and Privacy Commission, ID Support NSW, Police, Insurance providers, credit card companies etc
Preliminary Assessment of risk posed by the data breach? ○ High Risk (Established or suspected) = likely to result in serious harm to affected individuals/s or organisation ○ Moderate Risk ○ Low Risk

Data Breach Response Report

Name/Position:	Date:
List the response team members	
Listing of preliminary steps that have been taken to contain the breach	
Any further steps identified to minimise the impact on affected individuals or organisations?	
Validation of risk posed by the data breach. ○ High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation ○ Moderate Risk ○ Low Risk	
Confirmation of notification required ○ NDB Eligible data breach – mandatory disclosure (high risk) ○ Council elected voluntary disclosure (low or medium risk) ○ GDPR data breach – mandatory disclosure required within 72 hours (high, medium or low risk)	
Agencies notified ○ OAIC ○ NSW Information and Privacy Commission	
Confirmation of Notification Approach ○ Directly notify only those individuals at risk of serious harm, or ○ Directly notify all individuals whose data was breached, ○ Publicise the statement more broadly.	

Please specify whether notification is to occur via phone, letter, email or in person.
Next steps for Review phase

OAIC Four Step Response Plan

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.