Overview

The Notifiable Data Breaches (NDB) scheme went into force on February 22, 2018, under the federal *Privacy Act 1988* (Privacy Act). Under the NDB program, organisations and individuals must notify impacted persons as well as the Office of the Australia Information Commissioner (OAIC) and Information and Privacy Commission (IPC), NSW when a data breach is likely to result in substantial harm to an individual whose personal information has been compromised.

Along with the NDB program, the NSW Information and Privacy Commission must comply with the Commonwealth NDB scheme specifically in relation to breaches of tax file numbers (TFN). The introduction of the NSW Mandatory Notifiable Data Breach (MNDB) scheme aims to align with the Commonwealth NDB scheme and reduce inter-jurisdictional inconsistencies.

While the Commonwealth NDB scheme primarily targets Commonwealth government agencies and private sector organisations regulated by the APPs under the Privacy Act, there are provisions that also apply to NSW public sector agencies, especially regarding TFN breaches.

The Inverell Shire Council keeps records of individuals' personal information, including ratepayer, resident, and customer statistics and information. Additionally, the Council keeps track of employee and personal information. In order to plan, monitor, and manage the workforce, services, and properties throughout the Local Government Area (LGA), the Council gathers this data.

Given that the Council needs to use personal information to provide its services, Council must comply with the mandatory requirements of the Notifiable Data Breach scheme, which entails establishing a data breach notification protocol as required by the legislative changes set in November 2023, guiding the Council to exercise the utmost caution when handling personal information.

In the event that a data breach occurs, Council must abide by the scheme's notification requirements since failure to do so could subject Council to severe penalties under Australian law.

Scope

The purpose of this policy is to provide a procedure detailing the key actions and responsibilities to be followed in the event of a data breach incident. It makes use of the four crucial actions recommended by the OAIC and IPC for handling a data breach (see Appendix B).

The scope of this policy applies to all data held by Council in either a paper-based or electronic format and is applicable to all employees (including councilors, contractors, students, volunteers and agency personnel) as well as external organisations and contractors who have been granted access to Council's infrastructure, services and data.

This procedure supplements Inverell Shire Council's Privacy Management Plan.

Data Breach Management Plan

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, but not limited to:

- A device with a customer's personal information is lost or stolen.
- A database with personal information is hacked.
- Unauthorised use, access to or modification of data or information systems.
- Personal information is mistakenly given to the wrong person.
- Unauthorised disclosure of classified material or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the IPC website without consent.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

When do we know it has occurred?

Council may be made aware of a data breach through a complaint from a member of staff, a contractor, an impacted third party, or a report from another government department. A written request for an internal examination of a privacy complaint involving a data breach occurrence may also be sent to Council.

When does a breach become eligible for notification?

Affected persons, OAIC and IPC must be notified of a qualifying data breach under the Notifiable Data Breach (NDB) scheme.

A qualifying data breach happens when:

- Unauthorised access to, unauthorised disclosure of, or loss of personal information that a company or agency holds.
- Something that is likely to cause one or more people serious "harm".
- The company or agency hasn't been able to prevent the risk of serious harm with preventative measures.
- Government sector data has been exposed.
- Data breaches involving health records (within the meaning of the Health Records and Information Privacy Act 2002).

The following elements can be used to assess the "harm" produced by a breach and may be utilised to make a determination:

- Legal liability
- Financial loss
- Emotional wellbeing/loss
- Physical safety of the person/organisation
- Reputational damage
- Breach of secrecy provisions

An entity or agency that suspects an eligible data breach has occurred must analyse the situation as soon as possible to determine if it is likely to cause substantial harm to any individual.

NOTE: The relevant OAIC guidelines are available at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches; https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-data-breaches-involving-tax-file-numbers and provide further information on assessing an eligible breach.

Timeframe for assessing potential Data Breach

The Council is required to take all reasonable steps to complete the assessment within 30 calendar days of being aware of the qualifying data breach.

Where the Council is unable to reasonably complete an assessment within 30 days, the OAIC and IPC recommends that it document this so that it can demonstrate:

- That all reasonable steps were taken to complete the assessment within 30 days.
- The reasons for the delay.
- That the evaluation was reasonable and expeditious.

How to report a Data Breach?

A known or suspected data breach should be reported verbally or in writing to Manager Information Services as soon as possible, who will commence the response process.

Data Breach Response Process

1. Contain

- As soon as a suspected breach is reported, the Manager Information Services should gather the essential information and determine if a breach has occurred. If no breach is determined, complete a file note on the incident and advise the Director Corporate and Economic Services.
- If a breach occurred, complete the Data Breach Incident and Response Report - Part A (See Appendix A), notify the Director Corporate and Economic Services and keep any proof of the breach.
- Once the details of the incident have been gathered, the Manager Information Services should take the necessary steps to contain the breach (this may include coordinating with other staff members to ensure necessary steps/measures are put in place).
- Once a preliminary assessment of the level of risk posed by the breach (High, Medium, Low) has been established, notify the Response Team, and arrange a time to assess the breach.

2. Assess

- The Data Breach Response Team should evaluate the Manager Information Services preliminary evaluation and complete the Data Breach Incident and Response Report - Part B (See Appendix A).
- The following should be given special consideration because they will decide the implications for Council in terms of the notification process;

- Whether the violation is likely to cause serious harm to any affected parties

- Council may seek third-party help or advice from the NSW Information and Privacy Commission to provide an opinion or validate the Response Team's assessment.
- Any additional corrective actions identified by the Response Team to contain or mitigate the severity of the breach should be implemented.
- The assessment of the breach should be performed as soon as possible, but no later than 30 days after the breach is notified.

3. Notify

- After the Data Breach Incident and Response Report (See Appendix A) has been completed and reviewed by the Response Team, and it is determined that Council is legally required to provide notification of the incident, notification is expected to occur within 72 hours of the assessment.
- If required, the OAIC and the NSW Information and Privacy Commission should be notified.
    - OAIC - https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data- breach/
    - NSW Information and Privacy Commission. https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification

- Council must then notify individuals at risk of serious harm either;
    - directly notify only those individuals at risk of serious harm, or
    - directly notify all individuals whose data was breached,
- If the individuals affected are not known or can't be identified, then Council will;
    - Publicise the statement more broadly.
- The Manager Administrative and Marketing Services must be alerted in order to write a Media Statement in response to the data breach, if necessary.
    - Data Breach Incident and Response Report - Part B (See Appendix A) contains guidelines for notifying a breach. This should be used as a guideline when communicating breaches with individuals and in general.

4. Review

- Following the assessment of the incident and notification, the Manager Information Services should conduct a review within 14 days to identify any actions required to prevent further breaches, which should be tabled at the Management Team Meeting and include:

    - Recommended changes to system and physical security
    - Recommended suggestions for revisions to any Council policies or processes.
    - Staff training and education should be revised or changed.

5. Prevent

- Once immediate steps have been taken to mitigate the risks associated with a breach, the Council must take the time to investigate the cause of the breach.
- The Management Team must be briefed on the outcome of the investigation, including recommendations:

    - To make appropriate changes to policies and procedures if necessary.
    - Revise staff training practices if necessary.
    - Update this Response Plan if necessary.

Roles & Responsibilities

Staff in the following positions will typically make up the Data Breach Response Team:

Position	Responsibilities
General Manager (High Risk Only)	• General advice
Director Corporate and Economic Services	• General governance and advice • Process oversight, quality assurance • General advice and direct linkage to executives
Manager Information Services	• Compliance and records management advice and coordination of preliminary assessment and response team • Provide advice around application-level data/information security • Provide advice around technical/IT • infrastructure security
Manager Administrative and Marketing Services	• Communications advice
Legal Counsel (third party)	• Legal advice

The Response Team may also seek advice from 3rd Party privacy specialists or the NSW Information and Privacy Commission if deemed necessary as part of the assessment process.

References

This Data Breach Response Policy is based on the OAIC's Data breach notification: a guide to dealing with information security breaches, and the IPC Data Brach Guidance for NSW Agencies.

In the case of a data breach, the Response Team should refer to the Guide since it contains additional information that may be useful to the Response Team.

- https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
- https://www.ipc.nsw.gov.au/resources/ipc-data-breach-notification-form
- https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies
- https://www.ipc.nsw.gov.au/fact-sheet-notification-affected-individuals-data-breach
- https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-data-breaches-involving-tax-file-numbers
- https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements

Related Documents and Council Policy

- Inverell Shire Council Privacy Management Plan.
- Information and Privacy Commission Website.
- Office of the Australian Information Commissioner Website.

Related Legislation

- Privacy Act 1988 (Privacy Act).
- Privacy and Personal Information Protection Act 1998

Appendix

Appendix A – Data Breach Incident Report

Part A – Data Breach Incident Report

To be completed by the Manager Information Services (or his/her representative) on receipt of a breach report.

Name/Position:	Date:
When, where and how did the breach occur?	
Who and how was the breach discovered?	
When was the breach first reported to the Director Corporate & Community Services	
How would you classify the breach? • Unauthorised access • Unauthorised disclosure • Loss • Alteration • Destruction of personal information	What information/data has been compromised? • Financial details • Tax File Number • Identity Information • Contact Information • Health Information • Other
What parties have been affected by the breach?	
Steps taken to immediately contain the breach?	
Have any external parties been notified about the breach? E.g. The OAIC, NSW Information and Privacy Commission, 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 individual/s or organisation • Moderate Risk • Low Risk	

Part B – Data Breach Response Report

To be completed by the Manager Information Services at completion of the Response Team's assessment meeting.

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 o 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	

Appendix B – OAIC's – Four key steps to responding to data breaches

The following diagram provides an overview of a typical data breach response, including the requirements of the NDB scheme. This diagram is a summary and should be read with reference to the more detailed resources listed above.