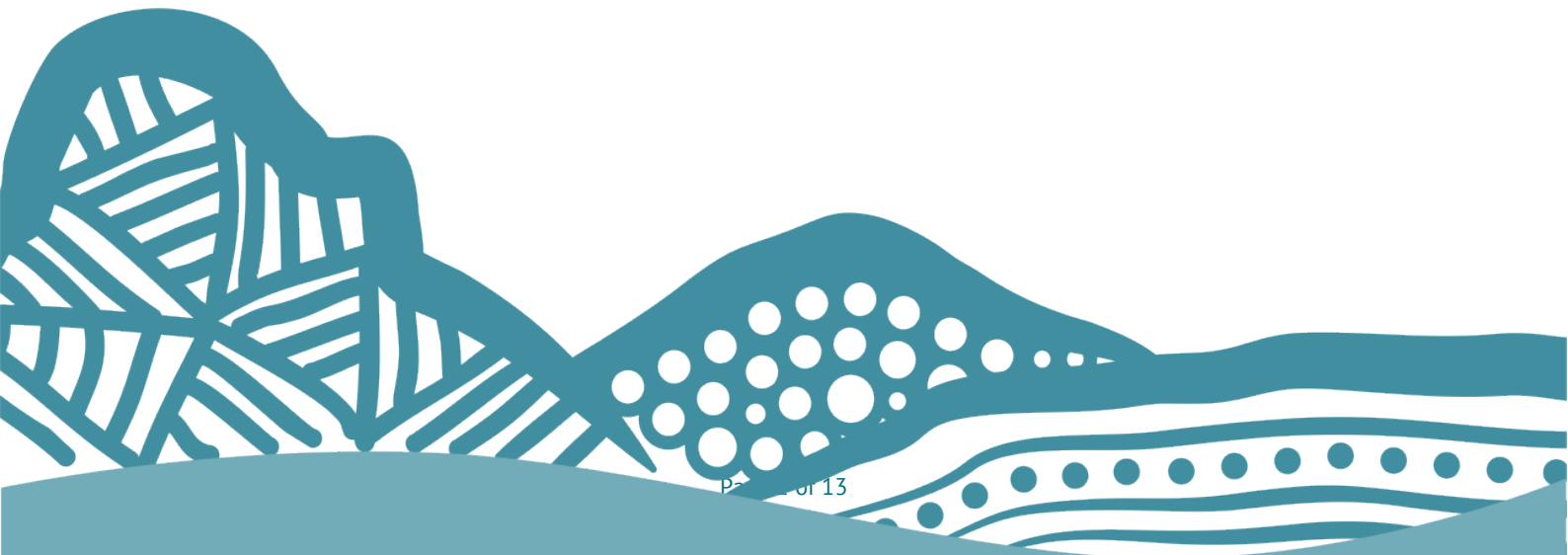




Kyogle Council

Data Breach Policy – 2024



Document History

Document Name: Kyogle Council –Data Breach Policy

Document Authority: Manager Information Technology

Date Adopted:

Document Reviews: Every Four Years

Version	Date	Details	Completed by
v0.1	26 March 2024	Initial Draft	Carol Ennis

Table of Contents

Document History	2
Purpose.....	4
Scope of Policy.....	4
Related Legislation and Documentation:.....	4
Definitions	5
Legislation.....	6
What is an eligible data breach?.....	6
Responding to a data breach	7
APPENDIX A – FACTORS TO CONSIDER IN ASSESSING SERIOUS HARM	10
APPENDIX B – CONTENTS OF A MANDATORY NOTIFICATION STATEMENT	12
APPENDIX C – HOW TO NOTIFY INDIVIDUALS.....	13

Purpose

This Data Breach Policy provides Kyogle Council with a strategy to handle incidents involving unauthorised access, disclosure, or loss of sensitive data, effectively and efficiently. The purpose of this policy is to minimise the impact of a data breach on Council, our customers, and stakeholders and to ensure Council reports data breaches in line with the Notifiable Data Breach Scheme – Privacy Act 1998, and to also assist in preventing any future breaches.

Scope of Policy

This policy applies to:

- Council employees
- Councillors

Related Legislation and Documentation:

- Privacy and Personal Information Protection Act 1998
- Notifiable Data Breach Scheme – Privacy Act 1998
- Privacy Act 1988 (Cth)

Kyogle Documents:

- Cyber Security Management Strategy
- IT Acceptable Use
- Privacy Management Policy
- Business Continuity Plan
- Kyogle Council - Data Breach Response Plan

Definitions

Term	Definition
Data breach	Unauthorised access to, unauthorised disclosure of, or loss of, personal information held by Kyogle Council.
Personal information As described in PPIP Act. 1998	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes, but is not limited to, information about Council employees, residents, ratepayers, suppliers, and other Council contacts. It can include details such as name, address, phone number, email address, date of birth, tax file number (TFN), ratepayer records, licence details, etc. Individuals may still be identifiable even when steps have been taken to de-identify information, e.g. removing direct identifiers or aggregating data. As such, it is prudent to treat de-identified information as personal information in the event of a data breach.
Notifiable data breach	Data breach that meets specific criteria, such as to trigger a legal requirement to notify the affected individuals and/or appropriate regulator.
Low-risk data breach	Loss or exposure of aggregated data only or of individual-level data in circumstances where it is reasonably believed that no real harm could occur. For example, paper files are left behind in a meeting but quickly retrieved.
Medium-risk data breach	Loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have malicious intent and that the data is somewhat protected. For example, a laptop with encrypted data is left on a bus.
High-risk data breach	Reasonably believed that the data breach is likely to result in serious harm to one or more of the individuals to whom the information relates. For example, cybercriminals breach Council's firewall and copy valuable customer data. This level of data breach is classified as a 'notifiable' data breach unless it falls under one of the exemptions to the notification rules.
Serious harm	Serious physical, psychological, emotional, financial, or reputational harm. For example, identity theft, financial loss or blackmail, threats to personal safety, loss of business or employment opportunities, humiliation, stigma, embarrassment, damage to reputation or relationships, discrimination, bullying, marginalisation, or other forms of disadvantage or exclusion.
Likely to result in serious harm	The risk of serious harm to an individual is more probable than not.
De-identification	A person's identity is no longer apparent or cannot be reasonably ascertained from the information or data.
PIPP Act.	Privacy and Personal Information Protection Act 1998.
IPC NSW	Information Privacy Commission NSW.
Business Continuity Plan	Kyogle Council's BCP defines any identified risks that can affect its business operations and what plans are in place to continue operating during an unplanned event.
TFN	Tax File Number

Legislation

Part 6a of the Privacy and Personal Information, Protection Act 1998 (NSW) (PPIP Act), establishes the NSW Mandatory Notification of Data breach (MNDB) Scheme¹. This scheme requires all public sector agencies to prepare and publish a Data Breach Policy (DBP) for managing such breaches and maintain an internal and public register of eligible data breaches.

What is an eligible data breach?

A data breach occurs when **personal information**² (defined in terms and definitions) held by Council (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

A data breach may occur as the result of:

- Systems failure
 - Equipment failure.
 - Software errors.
 - Applications and operating systems are not maintained through support patches.
- Human error
 - A letter/email sent to the incorrect recipient.
 - Incorrect system access granted to someone without appropriate access.
 - Lost or misplaced physical assets such as paper records, laptops, USB sticks, and mobile phones that contain personal information.
 - Failure to implement appropriate password security, password sharing.
- Malicious or criminal attack
 - Cyber incidents such as malware, phishing, denial of service attacks.
 - Social engineering or impersonation leading to inappropriate disclosure of personal information.
 - Insider threats using valid credentials to access or disclose personal information.
 - Theft of physical assets such as paper records, laptops, USB sticks, and mobile phones that contain personal information.

¹ Mandatory Notification of Data Breach Scheme <https://www.ipc.nsw.gov.au/privacy/MNDB-scheme>

² PPIP Act. Definition of personal information. <https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/ppip>

An **eligible**³ data breach under the MNDB Scheme applies when the following two tests are satisfied:

1. There is unauthorised access to, or unauthorised disclosure of **personal information** held by Council or there is a loss of **personal information** held by Council in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, **and**
2. 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.

Responding to a data breach

All staff, councillors, and contractors are responsible for notifying either the Manager Information Technology or the Executive Manager Corporate Services of any data breaches within one business day of becoming aware of a data breach. This will ensure the activation of the Data Breach Response Plan and allow for any subsequent advice to be provided to the Information Privacy Commissioner to assist in responding to enquiries made by the public and managing any complaints that may be received due to the breach.

There are four key steps for responding to a data breach:

1. **Contain** the breach and conduct a preliminary investigation.
2. **Evaluate** and mitigate the risks associated with the breach.
3. **Notify** and communicate.
4. **Review** the incident to prevent further breaches.

The first three steps are to be carried out concurrently where possible. The remaining step provides recommendations for longer-term solutions and prevention strategies.

1. **Contain the breach and conduct a preliminary investigation.**

- Immediately take all realistic steps to contain the breach and minimise any resulting damage.
- Conduct a preliminary investigation into the breach.
- Make a preliminary assessment of the risk posed by the breach.
- For “High” rated breaches, the Breach Response Team should immediately be activated to oversee the remainder of the breach response process.

³ IPC Data Breach policy – Eligible Data Breach definition. https://www.ipc.nsw.gov.au/sites/default/files/2023-10/IPC_Data_Breach_Policy_October_2023.pdf

2. Evaluate and mitigate the risks associated with the breach.

- As soon as practicable, take remedial action to prevent or lessen the likelihood that the breach will result in harm to any individual.
- Determine the type of data involved in the breach.
- Complete an assessment of the risk and potential for serious harm associated with the breach.
- Determine if the breach is an eligible breach under the MNDB Scheme

Factors to consider includes:

- **Who is affected by the breach?** The assessment will include reviewing whether individuals and organisations, how many individuals and organisations and whether individuals have been affected by the breach. And whether any of the individuals have personal circumstances which may put them at particular risk of harm.
- **What was the cause of the breach?** The assessment will review whether the breach occurred as part of a targeted attack or through inadvertent oversight.
 - Was it a one-off incident, or does it expose a more systemic vulnerability?
 - Has the data or personal information been recovered?
 - Is the data or personal information encrypted or otherwise not readably accessible?
- **What is the foreseeable harm to the affected individuals/organisations?** The assessment will include reviewing the possible use of the data or **personal information**.
 - Could it be used for identity theft, or lead to threats of physical safety, financial loss, or damage to reputation?
 - Who is the recipient?
 - What is the risk of further access, use or disclosure?

To mitigate the breach, Council will consider the following measures:

- Implementation of additional security measures within Council's own systems and processes.
- Limiting the dissemination of breached personal information.
- Engaging with relevant third parties to limit the potential for breached **personal information** to be misused for identity theft or other purposes or to streamline the re-issue of compromised identity documents. For example, contacting an identity issuer or financial institution.

3. Notify and communicate.

If an eligible data breach has occurred, the notification process under Division 3 of MNDB Scheme⁴ (Part 6A of the PPIP Act) is triggered.

1. Notify the Privacy Commissioner immediately after establishing an eligible data breach using the [approved form](#)⁴.
2. Determine if an [exemption](#)⁵ applies.

3. Notify individuals – unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.
4. Provide further information to the Privacy Commissioner as requested.
5. Add High Risk breaches to Council’s internal register of eligible data breaches.⁶

NOTE: if the data breach is not eligible under the MNDB Scheme, Council can still consider notifying affected individuals/organisations.

Other notifications to consider:

- NSW Police Force if the breach is suspected criminal activity.
- Cyber Security NSW, The Australian Cyber Security Centre, where the breach relates to a cyber security incident.
- Any third-party organisation or agencies whose data may be affected.
- Financial service providers, where a data breach includes an individual’s financial information.

4. Review the incident to prevent further breaches.

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

Preventative actions may include:

- Review IT systems and remedial actions to prevent future data breaches.
- Security audit of both physical and technical security controls.
- Review of policies and procedures.
- Review of employee/contractor training practices.
- Review of contractual obligations with contracted service providers.

⁴ Data Breach Notification to the Privacy Commissioner https://www.ipc.nsw.gov.au/sites/default/files/2023-07/Form_Data_Breach_Notification_to_the_Privacy_Commissioner_July_2023.pdf

⁵ IPC Fact Sheet – Exemptions from notification requirements. <https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements>

⁶ s.59ZE of PPIP Act.

APPENDIX A – FACTORS TO CONSIDER IN ASSESSING SERIOUS HARM

The **assessment** about the **likelihood of serious harm** should have regard to:

1. The **type of information** involved: for example,
 - a. Name and address
 - b. Financial
 - c. Health
 - d. Criminal records
 - e. Evidence of identify documents
 - f. Other unique identifiers, biometrics
 - g. Sensitive information e.g. person's ethnicity, religion or sexuality
2. The **volume of information** involved: is it a combination of pieces of data about a person which would not otherwise be known?
3. The **number of individuals** affected: for example, is there a risk that, due to the number of people impacted, there is a higher chance that someone in the cohort may experience serious harm as a result of the breach?
4. Whether the **information is protected** by one or more security measures: for example, the likelihood that any of the security measure could be overcome?
5. The **risk profile of the information** involved: for example, could it be used:
 - a. For identify theft or other fraudulent purposes?
 - b. To humiliate or blackmail?
 - c. To commit physical harm?
6. The **type of individuals** affected: for example, are the individuals:
 - a. Experiencing vulnerability (e.g. victims of family violence)?
 - b. Worth targeting in some way (e.g. very wealthy people or public figures)?
7. **How much time passed** between becoming aware of the data breach and containing it?
8. The **context**: was this an:
 - a. Isolated incident?
 - b. Systemic problem?
 - c. Deliberate attempt to steal data?
 - d. Result of an accident or other unintentional behaviour?
9. The **likelihood** that the persons who may have obtained the information have an intention to cause harm to any of the individuals affected by the data breach?
10. **Future breaches**: is there a risk of ongoing breaches or further exposure of the information?
11. The **risk of cumulative harm**: have there been breaches in other organisation that could result in a cumulative effect of more serious harm?
12. The **extent to which the risk has been successfully prevented** or lessened by remedial actions or containment efforts: for example, was the data encrypted, was the portable storage device remotely wiped, were the hard copy files quickly recovered?

13. Given all of the above, the **type of harm likely to affect the individuals**: for example,
- a. Identity theft
 - b. Financial loss
 - c. Threat to physical safety
 - d. Threat to emotional wellbeing,
 - e. Loss of job opportunities
 - f. Humiliation
 - g. Damage to reputation or relationships
 - h. Workplace or social bullying or marginalisation

APPENDIX B – CONTENTS OF A MANDATORY NOTIFICATION STATEMENT

The mandatory notification statement to impacted individuals must set out the following:⁷

- the date the breach occurred,
- a description of the breach,
- how the breach occurred,
- the type of breach that occurred (i.e. unauthorised disclosure, unauthorised access, loss of information),
- the personal information that was the subject of the breach,
- the amount of time the personal information was disclosed for,
- actions that have been taken or are planned to secure the personal information is secure, or to control and mitigate the harm done to the individual,
- recommendations about the steps the individual should take in response to the data breach (e.g. link to www.idcare.org if the breach suggests assistance should be provided to protect individuals against identity theft),
- information about making privacy-related complaints and internal reviews of certain conduct of public sector agencies,
- the name and contact details of the public sector agency subject of the breach, if more than one public sector agency was subject of the breach, the name of each other agency.

The mandatory notification statement to the IPC must be via the [approved form](#)⁸, and must set out:

- the information provided to impacted individuals (see above),
- a description of the personal information that was the subject of the breach,
- whether the head of the agency is reporting on behalf of other agencies involved in the same breach,
- if the head of the agency is reporting on behalf of other agencies involved in the same breach, the details of the other agencies,
- whether the breach is a cyber incident,
- if the breach is a cyber incident, details of the cyber incident,
- the estimated cost of the breach to the agency,
- the total number, or estimated total number, of individuals affected or likely to be affected by the breach, and notified of the breach,
- whether the individuals notified have been advised of the complaints and internal review procedures under the PPIP Act.

⁷ s.590 PPIP Act.

⁸ s.59M(2) PPIP Act; see also the template form at https://www.ipc.nsw.gov.au/sites/default/files/2023-07/Form_Data_Breach_Notification_to_the_Privacy_Commissioner_July_2023.pdf

APPENDIX C – HOW TO NOTIFY INDIVIDUALS

There are three options for notifying individuals at risk of serious harm, depending on what is 'practicable':

1. Directly notify only those individuals at risk of serious harm, or
2. Directly notify all individuals whose data was breached, or
3. Publicise the statement more broadly.

ID Support NSW can assist Council to identify and notify affected individuals.

1. Where it is possible to identify and contact only those individuals at risk of serious harm, Council must directly notify those individuals. Secondly, Council may, but is not obligated to, publish the notification more broadly e.g. on Council's website or via social media.
2. Where it is not possible to identify which individuals might be at risk of serious harm, but it is possible to directly contact all individuals whose data was breached, the Council will directly notify all individuals whose data was breached. Secondly, Council may, but is not obligated to, publish the notification more broadly e.g. on Council's website or via social media.
3. Where it is not reasonably practicable to identify which individuals might be at risk of serious harm, and it is not reasonably practicable to directly contact all individuals whose data was breached (e.g. if the contact details are not current), then Council **MUST** publish a notification on their website, in a 'public notification register'.⁹ Council must also take reasonable steps to publicise that notification, e.g. consider other methods of communication such as social media, newspaper advertisement.

⁹ s.59P PPIP Act. Council's 'public notification register' must be available for at least 12 months, and the IPC must be informed of its existence.