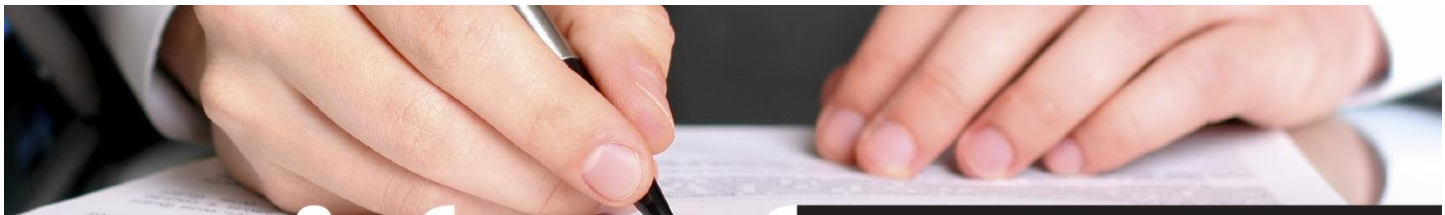

PRIVACY MANAGEMENT PLAN

DATE ADOPTED: 24 OCTOBER 2023

VERSION: 5.0

POLICY OBJECTIVES

The objective of the Privacy Management Plan ('Plan') is to:

- Establish practices and procedures to protect the privacy rights of individuals with respect to all forms of personal and health information held by Maitland City Council.
- Specify how Maitland City Council handles the personal and health information it collects, stores, accesses, uses and discloses in the course of its business activities.
- Ensure Maitland City Council complies with the principles and requirements of the *Privacy and Personal Information Protection Act 1998* (NSW) ('PPIP Act'), the *Health Records and Information Privacy Act 2002* (NSW) ('HRIP Act'), and the Privacy Code of Practice for Local Government ('privacy obligations').

POLICY SCOPE

The privacy obligations and this Plan apply to the General Manager, Councillors, staff, contractors, volunteers, and committees of Maitland City Council.

Council will take reasonable steps to ensure that all such parties are made aware that they must comply with the privacy obligations and this Plan.

POLICY STATEMENT

Maitland City Council is committed to appropriately handling, managing, and protecting the personal and health information it collects and holds.

As a public sector agency, Council is required to have a privacy management plan in accordance with section 33 of the PPIP Act.

This plan addresses particular matters that affect personal information collected and held by Maitland City Council and provides Council staff with guidance on the privacy obligations and sets out practices and procedures which have been adopted to minimise the risk of inappropriately releasing personal information and non-compliance whilst still enabling Council to conduct its functions.

1. PERSONAL AND HEALTH INFORMATION

1.1. What is personal information?

Personal information is defined in section 4 of the PPIP Act as:

'Information or opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or could reasonably be ascertained from the information or opinion'.

1.2. What is not personal information?

Personal information does not include:

- Information about an individual that is contained in a publicly available publication, such as:
  - Personal information in a newspaper, magazine, book, or advertisement that is distributed broadly to the public,
  - Personal information on the internet,
  - Personal information in Council business papers that are available to the public; and
  - Personal information on electoral rolls.
- Information about an individual who has been deceased for more than 30 years.
- Information about an individual that is contained in a public interest disclosure or collected in the course of an investigation arising out of a public interest disclosure within the meaning of the *Public Interest Disclosures Act 2022 (NSW)*.

1.3. What is health information?

Health information, as defined in section 6 of the HRIP Act, includes personal information that is information or an opinion about the physical or mental health or a disability (at any time) of an individual. Health information also includes personal information that is information or an opinion about:

- A health service provided, or to be provided, to an individual
- An individual's express wishes about the future provision of health services to him or her
- Other personal information collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances (e.g., blood test, x-ray, psychological report, results from drug and alcohol tests)
- Genetic information that is or could be predictive of the health of an individual or their relatives or descendants.

1.4. Examples of personal and health information

Council holds personal and health information concerning its customers, ratepayers, and residents such as:

- Names, home addresses, and telephone numbers of individuals
- Property ownership details and information regarding concessions
- Personal information relevant to the processing of development applications
- Information concerning contact with Council regarding provision of services including the completion of application forms and lodging of customer service requests.
- Bank account details of debtors and creditors to Council
- Children and young people attending Council events (such as vaccination programs)

Council holds personal information concerning Councillors such as:

- Personal contact information
- Complaints and conduct matters
- Pecuniary interest returns
- Entitlements to fees, expenses, facilities and reimbursements including bank account detail

Council holds personal and health information concerning its employees such as:

- Information acquired in the course of recruitment and selection including criminal history check, bankruptcy check, and pre-employment medical assessment
- Training and qualifications
- Working with children checks
- Leave and payroll data
- Personal contact information
- Emergency contact details
- Performance management plans
- Disciplinary matters
- Pecuniary interest returns
- Wage and salary entitlements and payments including bank account details
- Workers compensation claims, medical certificates, and injury documentation

Council holds personal and health information concerning its volunteers such as:

- Personal contact information
- Training and qualifications e.g., Responsible Service of Alcohol for events
- Working with children checks
- Type of volunteer
- Emergency contact details
- Volunteer application forms

2. ROLES AND RESPONSIBILITIES

2.1. General Manager

The General Manager is responsible for ensuring that Council complies with its obligations under the PPIP Act, HRIP Act, and this Plan.

2.2. Privacy Officer

The Manager Governance and Risk is Council's Privacy Officer.

The Privacy Officer is responsible for:

- Assisting the General Manager to ensure Council's compliance with obligations under the PPIP Act, HRIP Act, and this Plan.
- Creating awareness of this Plan.
- Coordinating steps to ensure Council complies with the PPIP Act and HRIP Act.
- Coordinating requests for the suppression of personal information.
- Coordinating requests for and undertaking internal reviews, including liaising with the NSW Privacy Commissioner regarding internal reviews.
- Providing advice on matters relating to privacy and personal information.
- Reviewing and updating this Plan.
- Ensuring this plan is made publicly available on Council's website and staff intranet.

2.3. All Staff

All Council staff, councillors, contractors, volunteers, and committee members are responsible for:

- Collecting, storing, accessing, and disclosing personal information in accordance with this Plan and clauses relating to personal information in Council's Code of Conduct.
- Always including privacy disclaimers when collecting personal information
- Undertaking relevant training as required to use this Plan and comply with privacy obligations.
- Seeking advice from the Privacy Officer if they are unsure about a privacy issue.
- Not committing any offences under the PPIP Act and HRIP Act.

3. PUBLIC REGISTERS

Council is required under various Acts to maintain a number of public registers and to make them available for public inspection. A public register is a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee). Council is required to ensure that any access to personal information in a register is consistent with the purpose for which the register exists.

A detailed list of registers and access provisions can be found in Council's *'Right to Information Guidelines'*, available on Council's website.

3.1. Disclosure of personal information contained in public registers

Council will not disclose personal information kept in public registers unless Council is satisfied that the information is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

3.2. Application to access records on a public register

Under section 57 of the PPIP Act, before disclosing personal information contained in a public register, Council must be satisfied that the individual requesting access to the personal information intends to use the information for a purpose relating to the purpose of the register or the Act under which the register is kept.

An individual may request access to personal information contained in a public register by completing and submitting an *'Application for Access to Personal Information Form'* on Council's website.

Upon receipt of the completed application form, Council will provide without excessive delay and expense details of the personal information it holds that relate to that individual. The application will be processed within 20 working days.

Council can determine to provide a copy of the whole or part of a register depending on whether such disclosure fits with the purpose for which it was collected.

4. SUPPRESSION OF PERSONAL INFORMATION

In certain circumstances a person may request the suppression of their personal information held in a public register in accordance with Section 58 of the PPIP Act, and from any other document or record held by Council.

A person may request Council to not publish their personal information if they consider that the safety or wellbeing of a person would be affected by the information being placed on the public register or released by Council. Council will suppress the information in accordance with the request unless Council is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information. When in doubt, Council will favour suppression. Any information that is sup-pressed from the public register may still be kept for other purposes.

An application for suppression should be made in writing and addressed to Council's Privacy Officer stating the reasons for the request. The Council may require additional supporting documentation where appropriate.

5. INFORMATION PROTECTION PRINCIPLES AND HEALTH PRIVACY PRINCIPLES

Council must comply with the 12 Information Protection Principles ('IPP') contained in Part 2, Division 1 of the PPIP Act, and the 15 Health Privacy Principles ('HPP') contained in Schedule 1 of the HRIP Act. An overview of the principles as they apply to Council is included below.

5.1. IPP 1 & HPP 1 – Lawful collection

Council will not collect personal or health information by any unlawful means. Council will only collect personal or health information reasonably necessary for a lawful purpose directly related to a function or activity of the Council and necessary for that purpose. The *Local Government Act 1993* (NSW) and other relevant Acts govern the functions and activities carried out by Council.

Council will collect and deliver personal information to and from government departments involved in the normal functions of Council's operations.

Council will collect information:

- Verbally (e.g., face to face in meetings, over the counter or on the phone)
- Via forms completed by individuals
- By correspondence both electronically and in physical form
- From Government and non-government agencies

5.2. IPP 2 & HPP3 – Direct collection

When collecting personal information Council will collect personal information directly from the individual to whom the information relates, unless the individual has authorised collection from someone else or the information has been provided by a parent or guardian of a person under the age of 16 years or is incapacitated by disability or age.

5.3. IPP 3 & HPP 4 – Requirements when collecting information

When collecting information from an individual Council will take reasonable steps to ensure the individual is notified of:

- The fact that information is being collected
- The purpose for which the information is collected
- The intended recipients of the information
- Whether the supply of information is required by law or is voluntary, and the consequences for the individual if the information (or any part of it) is not provided
- The existence of any right of access to and correction of the information
- Council's name and address where the information will be stored

Where practicable, a privacy protection notice will be included on any forms where Council is collecting personal or health information. If health information is collected about an individual from someone else, reasonable steps must be taken to ensure that the individual has been notified, unless making the individual aware would impose a serious threat.

5.4. IPP 4 & HPP 2 – Other requirements for collection

Council will take reasonable steps to ensure that:

- Information collected is relevant to a purpose, is not excessive, and is accurate, up to date and complete
- The collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

The exemption to this relevance is for information collected by CCTV per section 9 of the PPIP Regulation.

5.5. IPP 5 & HPP 5 – Retention & security

Council will ensure:

- That personal and health information is stored securely.
- That personal and health information is used for a lawful purpose and is kept for no longer than required
- That personal and health information will be disposed of securely and in accordance with the *State Records Act 1998 (NSW)*.
- Reasonable steps are taken to protect personal and health information against loss, unauthorised access, use, modification, or disclosure and against all other misuse.
- If it is necessary to release the information to a person in connection with the provision of a service of Council, everything reasonable is done to prevent unauthorised use or disclosure of the information and the owner of the information is consulted and informed of any such release in accordance with the abovementioned Acts.

The disposal of Council records is carried out in accordance with the State Records Act 1998 (NSW), the NSW General Disposal Authority for Local Government (GA39) and Council's Records Management Policy.

5.6. IPP 6 & HPP 6 – Information held by agencies

Council will take all reasonable steps to enable a person to determine whether Council holds personal or health information about them and upon such request Council will advise the person of the:

- Nature of that information
- The main purpose for which the information is held
- The persons entitlement to access that information

These Principles are subject to the *Government Information (Public Access) Act 2009* (NSW).

Note: Broad categories of personal and health information held by the Council are referred to in section 1.4 of this Plan.

5.7. IPP 7 & HPP 7 – Access to own information

At the request of an individual, Council will provide, without excessive delay and expense, details of the personal and/or health information it holds that relates to that individual.

To determine if Council holds personal or health information about them a person may complete an *'Application for Access to Personal Information'* form on Council's website.

The application will be processed within 20 working days.

Current staff can enquire with the Human Resources team to access their personnel records. Past employees will be required to submit a formal access to information application in accordance with Council's Right to Information Policy.

5.8. IPP 8 & HPP 8 – Alteration of information

Any person who is concerned with the inaccuracy or unacceptable use of their personal or health information kept by Council may request, in writing, for amendments to be made to that information.

Requests to alter personal or health information must be made using the *'Application for Alteration to Personal Information'* form available on Council's website. This request should be accompanied by appropriate evidence to support the making of an amendment that is sufficient to satisfy the Council that the amendment is factually correct and appropriate.

Council has an obligation to take steps to amend (whether by way of corrections, deletions, or additions) personal and health information where appropriate to ensure the personal and health information is accurate, relevant, up to date, not misleading and having regard to the purpose for which it was collected.

If Council decides that it will not amend the information it must, if requested by the individual concerned, take such steps as are reasonable to add the additional information enabling it to be read with the existing information and notify the individual concerned.

The individual to whom the information relates is entitled, if it is reasonably practicable, to have the recipients of the information notified of the amendments made by Council.

Incorrect records will be physically altered; whether computerised or in hard copy format.

Council's Privacy Officer will approve the required changes where applicable.

5.9. IPP 9 & HPP 9 – Accuracy of information

Prior to use or disclosure, Council will take reasonable steps to ensure that personal and health information is relevant, accurate, up to date, complete and not misleading. In doing so, Council will have regard to the purpose for which the information was collected and its proposed use.

5.10. IPP 10 & HPP 10 – Limits on use of information

Council will not use personal or health information for a purpose other than for that which it was collected unless:

- The individual to whom the information relates has consented to the use of the information for that other purpose
- The other purpose for which the information is used is directly related to the purpose for which it was collected
- The use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person

Some information collected by Council may be used for a variety of purposes. For example, the names and addresses of individual owners of property kept as part of Council's rates records may be used to notify adjoining owners of proposed developments, to identify companion animal ownership, evaluate land dedications and laneway status and to notify residents and ratepayers of Council services and activities. Individuals will not be notified for the use of personal information by Council staff to perform Council functions.

Personnel, health and recruiting records will only be released to the individual to whom the information relates as well as appropriate staff performing Council functions for which the information is held. Personnel information may only be released on the written authority of the individual staff member concerned.

5.11. IPP 11 and HPP 11 – Limits on disclosure of information

Council will not disclose personal information unless:

- The disclosure is directly related to the purpose for which it was collected and there is no reason to believe the individual concerned would object to the disclosure
- The individual has been made aware that this kind of information is usually released
- Disclosure is necessary to prevent or lessen a serious or imminent threat to the life of the individual concerned or another person

Members of the public can apply to access personal information held by Council that is not their own personal information under the *Government Information (Public Access) (GIPA) Act 2009 (NSW)*. For further information please refer to Council's Right to Information Policy and Guidelines.

Council will only disclose health information in the following circumstances:

- With the consent of the individual to whom the information relates
- For the purpose for which the health information was collected or a directly related purpose that the individual to whom it relates would expect
- If an exemption applies

5.12. IPP 12 – Special restrictions on disclosure of personal information

Council will take reasonable care not to disclose personal information that:

- Relates to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person
- Relates to an enquiry from anyone outside the State of NSW or to a Commonwealth agency unless:
    - A relevant privacy law applies to personal information in force in that jurisdiction
    - The disclosure is permitted under a privacy code of practice (a law determined by the Privacy Commissioner and published in the Government Gazette)

5.13. Further Health Information Privacy Principles

To the extent that Council collects personal health information in respect of an individual, Council will adhere to the 15 Health Privacy Principles as detailed in Schedule 1 of the Health Records and Information Privacy Act 2002. The following lists the additional health privacy principles which do not directly correlate with an information protection principle.

5.14. HPP 12 – Identifiers

Council will only give an identification number to health information if it is reasonably necessary for Council to carry out its functions effectively.

5.15. HPP 13 - Anonymity

Where it is lawful and practical Council will give individuals the opportunity to remain anonymous when receiving health services in conjunction with Council.

5.16. HPP 14 – Transborder data flow

Council will only transfer health information outside of NSW if the requirements of health protection principle 14 are met.

5.17. HPP 15 – Linkage of health records

Council will only include health information in a system to link health records across more than one organisation if the individual to whom the health information relates gives their express consent to the link.

6. EXEMPTIONS

Part 2, Division 3 of the PPIP Act contain specific exemptions from compliance with the above-mentioned principles in certain circumstances. These exemptions include:

- Section 23 – exemptions relating to law enforcement and related matters
- Section 23A – exemptions relating to ASIO
- Section 24 – exemptions relating to investigative agencies
- Section 25 – exemptions when non-compliance is lawfully authorised or required
- Section 26 – exemptions where non-compliance would benefit the individual – including when compliance would cause prejudice and consent to non-compliance
- Section 27 – exemptions relating to certain law enforcement agencies
- Section 27A – exemptions relating to information exchanges between public sector agencies

Further to the above statutory exemptions, the Privacy Code of Practice for Local Government also makes provisions for non-compliance with the principles in certain circumstances. For example, allowing the indirect collection of information which is reasonably necessary when an award, prize, benefit or similar form of recognition is intended to be conferred upon the person to whom the information relates.

7. MANDATORY NOTIFICATION OF A DATA BREACH

The PPIP Act, incorporates a Mandatory Notification of Breach ('MNDB') Scheme that requires Council to notify the NSW Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

Council has developed a Data Breach Policy and Data Breach Response Plan (included at Appendix 1 of this Plan) that sets out how Council will respond to a data breach.

7.1. What is a data breach?

A data breach occurs when personal information 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.

This may or may not involve disclosure of personal information external to Council or publicly. For example, unauthorised access to personal information by a Council staff member, or unauthorised sharing of personal information between teams within Council may constitute a data breach.

A data breach may occur as the result of malicious action, systems failure, or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles ('IPPs').

Examples of when a data breach may occur include:

- When a letter or email containing personal information is sent to the wrong recipient.
- When a physical asset like a laptop or USB stick containing personal information is lost, misplaced, or stolen.
- Cyber incidents such as ransomware, malware, hacking or phishing.
- Where a coding error allows access to a system without authentication.
- Insider threats from employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

8. COMPLAINTS AND INTERNAL REVIEW

8.1. Individuals right to internal review

Individuals have a right to request an internal review under Part 5 of the PPIP Act if they are aggrieved by the conduct of Council. 'Conduct' can mean an action, a decision, or even inaction by Council, such as:

- Perceived contravention of a privacy or health principle that applies to Council
- Perceived contravention of a code of practice that applies to Council
- Disclosure of personal information kept on a public register

8.2. Internal review process

A request for internal review must be made in writing and addressed attention to the Privacy Officer through the following channels:

- Email: info@maitland.nsw.gov.au
- Post:

The Privacy Officer
Maitland City Council
PO Box 220
Maitland NSW 2320

The Privacy Internal Review Form (Information and Privacy Commission) can be used.

On receipt of the internal review request, Council will forward a copy to the NSW Privacy Commissioner. Council will inform the NSW Privacy Commissioner of progress and the outcome of the review.

An application for internal review must be lodged within six months from the time the applicant first became aware of the conduct which is the subject of the internal review application.

At all times the content of the review will be kept confidential.

The internal review will be conducted by the Privacy Officer, or an appropriately qualified staff of Council, who does not have a conflict of interest.

The review will be completed as soon as reasonably practicable within 60days from the receipt of the application for review.

Following completion of the review Council will do one or more of the following:

- Take no further action on the matter
- Make a formal apology to the applicant
- Take appropriate remedial action
- Provide undertakings that the conduct will not occur again
- Implement administrative measures to ensure that the conduct will not occur again

As soon as practicable within 14 days of the completion of the review Council will notify the applicant in writing of:

- The outcome and reasons for the decision
- Any proposed actions to be taken
- The right of the applicant to have those findings and the Council's proposed action reviewed by the Administrative and Equal Opportunity Division of the NSW Civil & Administrative Tribunal.

8.3. External review

If the applicant is not satisfied with the outcome of an internal review, they can apply to the NSW Civil and Administration Tribunal ('NCAT') for an external review. An applicant has 28 days from the date of the internal review decision to seek a review by NCAT.

To request an external review, you must apply directly to the Administrative and Equal Opportunity Division of the NCAT, which has the power to make binding decisions on an external review. Contact details provided below:

Website:	www.ncat.nsw.gov.au
Email:	aeod@ncat.nsw.gov.au
Phone:	1300 006 228
Post:	PO Box K1026, Haymarket NSW 1240
Office address:	Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

8.4. Role of the NSW Privacy Commissioner

The NSW Privacy Commissioner's functions include:

- Promoting the adoption and monitoring the compliance with the privacy and health principles
- Preparing guidelines in respect of privacy matters
- Providing advice and conducting research on the protection of personal information and the privacy of individuals
- Receiving and investigating complaints about privacy related matters – complaints can be lodged directly with the NSW Information and Privacy Commission instead of to Council.

9. OFFENCES

Part 8 of the Privacy and Personal Information Protection Act 1998 NSW and the Health Records and Information Privacy Act 2002 NSW contain offences for certain conduct of public sector officials and other persons. For example, there are offences relating to corrupt disclosure and use of personal and health information by public sector officials, inappropriately offering to supply personal or health information that has been disclosed unlawfully, and wilfully obstructing or hindering the Privacy Commissioner or their employees from performing their role.

Section 664 of the *Local Government Act 1993* (NSW) makes it an offence for anyone to disclose information except in accordance with that section.

Contravention of privacy obligations and this Plan will be investigated, and staff may be subject to disciplinary action.

10. TRAINING AND EDUCATION

Appropriate training and/or briefings will be provided on a periodic basis and on induction to staff and councillors on our privacy obligations. This training will be supplemented by resources available on the staff intranet.

Council's Privacy Officer will be available to provide assistance and advice to staff on privacy matters as and when required.

11. REVIEW AND REPORTING OF THIS PLAN

This Plan will be reviewed every three years, or earlier if required by any legislative change, or to enhance the application of the legislation and/or regulations supporting this Plan.

A copy of this Plan will be provided to the NSW Privacy Commissioner as soon as practicable after the Plan is amended, as required under section 33(5) of the PPIP Act.

12. ACCESSIBILITY OF THIS PLAN

This Plan will be made publicly available on Council's website and staff intranet.

13. FURTHER INFORMATION

For assistance in understanding the process associated with the PPIP Act and the HRIP Act, the following organisations can be contacted:

Maitland City Council
Privacy Officer
PO Box 220
Maitland NSW 2320

Phone: (02) 4934 9700
Email: info@maitland.nsw.gov.au
Website: www.maitland.nsw.gov.au

Information and Privacy Commission NSW
GPO Box 7011
Sydney NSW 2001

Phone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NSW Civil and Administrative Tribunal – Administrative and Equal Opportunity Division
Level 10 John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000

Phone: 1300 006 228
Website: www.ncat.nsw.gov.au

DEFINITIONS

Affected individual	As defined in section 59D of the PPIP Act, an affected individual is an individual: • to whom the information subject to unauthorised access, unauthorised disclosure or loss relates, and • who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.
Data breach	Data breach means unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information. Examples of a data breach are when a device containing personal information is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person.
Data Breach Response Team	Team of assessors assigned to investigate and manage Council's response to a data breach as outlined in the Data Breach Response Plan. The General Manager will determine if a Data Breach Response Team is to be convened and select the members of the Data Breach Response Team. A member of the Data Breach Response Team may be: • An officer or employee of Maitland City Council, or • An officer or employee of another public sector agency acting on behalf of Maitland City Council, or • A person acting on behalf of Maitland City Council, or a person employed by that person (e.g., an individual employed by a third party to carry out the assessment for Maitland City Council). • To the exclusion of any person the General Manager reasonably suspects was involved in an act or omission that led to the data breach.
Eligible data breach	As defined in section 59D of the PPIP Act, 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.

Health information	A specific type of personal information which may include information or an opinion about the physical or mental health or a disability (at any time) of an individual. This includes, for example, information contained in medical certificates, information about medical appointments or test results.
Investigative agency	As defined by section 3 of the PPIP Act and includes the Ombudsman's Office and the Independent Commission Against Corruption.
Loss	Loss refers to the accidental or inadvertent loss of personal information held by Council, in circumstances where is it is likely to result in unauthorised access or disclosure. For example, where a staff member leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.
Personal information	Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or could be reasonably ascertained from the information or opinion, as defined in section 4 of the PPIP Act. For the purpose of this policy, personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002*.
Public data breach notification	Notification made to the public at large rather than a direct notification to an identified individual.
Public register	A public register is defined in section 3 of the PPIP Act as a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee).
Serious harm	Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the affected individual. That is, the effect on the individual must be more than mere irritation, annoyance, or inconvenience. Harm to an individual includes physical harm, economic, financial, or material harm, emotional or psychological harm; reputational harm, and other forms of serious harm that a reasonable person in Council's position would identify as a possible outcome of the data breach.
Unauthorised access	Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking). For example, a staff member browses a fellow employee's personnel record without any legitimate purpose.

Unauthorised disclosure	Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the organisation, and releases that information from its effective control in a way that is not permitted by the PPIP Act. This includes an unauthorised disclosure by an employee of the organisation. For example, a staff member accidentally publishes a confidential data file containing the personal information of one or more individuals on the internet.

POLICY ADMINISTRATION

BUSINESS GROUP:	Strategy, Performance and Business Systems
RESPONSIBLE OFFICER:	Group Manager Strategy, Performance and Business Systems
COUNCIL REFERENCE:	Ordinary Council Meeting 24 October 2023 – Item 11.1
POLICY REVIEW DATE:	Three (3) years from date of adoption
FILE NUMBER:	35/62
RELEVANT LEGISLATION	• Government Information (Public Access) Act 2009 (NSW) • Government Information (Public Access) Regulation 2018 (NSW) • Health Records & Information Privacy Act 2002 (NSW) • Health Records & Information Privacy Regulation 2022 (NSW) • Local Government Act 1993 (NSW) • Local Government (General) Regulation 2021 (NSW) • Privacy Act 1988 (Cth) • Privacy Code of Practice for Local Government • Privacy & Personal Information Protection Act 1998 (NSW) • Privacy & Personal Information Protection Regulation 2014 (NSW)
RELATED POLICIES / PROCEDURES / PROTOCOLS	• Data Breach Policy • Code of Conduct • Records Management Policy • Right to Information Policy • Right to Information Guidelines

POLICY HISTORY

VERSION	DATE APPROVED	DESCRIPTION OF CHANGES
1.0	June 2000	New policy adopted
2.0	25 February 2006	Updates to include requirements under Health Records & Information Privacy Act 2002.
3.0	26 February 2013	Policy updated to align with Information & Privacy Commissioner Guidelines.
4.0	28 June 2016	Policy updated to align with the Office of Local Government's Model Privacy Management Plan for Local Government
5.0	24 October 2023	Periodic review. Updates include amendments to ensure compliance with PPIP Act and HRIP Act, addition of Data Breach Response Plan at Appendix 1 to comply with the mandatory notification provisions under Part 6A of the PPIP Act, and inclusion of the Roles and Responsibilities section.

APPENDIX 1 – DATA BREACH RESPONSE PLAN

1. PURPOSE

The Data Breach Response Plan ('Plan') sets out the roles and responsibilities of Maitland City Council ('Council') staff in the event Council experiences a data breach, or suspects that a data breach has occurred.

The Plan also outlines the process established by Council to identify, contain, assess, and manage a data breach and, where considered an eligible data breach, notifying the NSW Privacy Commissioner and affected individuals.

This Plan should be read in conjunction with Council's Breach Data Policy.

2. ROLES AND RESPONSIBILITIES

2.1. GENERAL MANAGER

The General Manager is responsible for:

- Ensuring that Council is compliant with all relevant laws and regulations.
- Determining whether a Data Breach Response Team is to be convened and selecting the members of the Data Breach Response Team.
- Approving an extension of time to conduct the assessment of a suspected data breach.
- Determining whether the data breach is eligible for external notification.
- Undertaking external notifications to the NSW Privacy Commissioner and affected individuals/organisations.
- Notifying the NSW Privacy Commissioner of any further information and when an extension of time to the assessment period has been approved.
- Notifying Council's insurers as required.

2.2. GROUP MANAGER STRATEGY, PERFORMANCE AND BUSINESS SYSTEMS

The Group Manager Strategy, Performance and Business Systems is responsible for:

- Having an approved Data Breach Policy and Data Breach Response Plan in place to manage Council's data breach response.

2.3. EXECUTIVE MANAGER DIGITAL TRANSFORMATION

The Executive Manager Digital Transformation is responsible for:

- Taking action to respond to the actual or suspected data breach in accordance with the Data Breach Response Plan.
- Implementing any longer terms actions to contain and response to security threats to Council's ICT systems and infrastructure.

2.4. PRIVACY OFFICER

The Manager Governance and Risk is Council's Privacy Officer.

The Privacy Officer is responsible for:

- Receiving and assessing reports of actual or suspected data breaches.
- Initiating the Data Breach Response Plan.
- Preparing an initial data breach assessment report, including advice for the General Manager to determine if a Data Breach Response Plan is to be convened.
- Investigating and managing Council's response to a data breach where it is determined that a Data Breach Response Team is not necessary.

- Reviewing and updating the Data Breach Policy and Data Breach Response Plan.
- Planning, initiating, overseeing, and reporting on the testing of the Data Breach Policy and the Data Breach Response Plan.

2.5. DATA BREACH RESPONSE TEAM

The Data Breach Response Team is responsible for:

- Assembling promptly to investigate and manage Council's response to a data breach in accordance with the Data Breach Response Plan.
- Preparing advice for the General Manager to determine if the data breach is eligible for external notification.

2.6. VENDORS/THIRD PARTIES

Vendors/Third Parties are responsible for:

- Immediately notifying Council of any actual or suspected data breaches affecting Council.
- Having appropriate security measures in place to protect any personal information it collects or manages on behalf of Council.

2.7. ALL STAFF

All Council staff, councillors, contractors, and volunteers are responsible for:

- Immediately reporting any actual or suspected data breaches to the Privacy Officer.
- Undertaking required training relating to privacy, PPIP Act requirements, and Council's data breach response process.
- Complying with the Data Breach Policy and the Data Breach Response Plan.

2.8. MEMBERS OF THE PUBLIC

Members of the public outside of Council can report an actual or suspected data breach affecting Council.

3. REPORTING A SUSPECTED DATA BREACH

Any Council staff member, councillor, contractor, volunteer, third party, or member of the public with reasonable grounds to suspect that a data breach has occurred should immediately report the suspected breach to Council's Privacy Officer (info@maitland.nsw.gov.au), providing as much information as you can about the suspected data breach.

Refer to Section 4.1 of this Plan for what information to include in your report.

You should also notify your direct supervisor of the suspected data breach; vendors and any other third parties should also notify their primary contact person at Council.

4. DATA BREACH RESPONSE PLAN

Council's Data Breach Response Plan comprises of the following steps:

1. INITIAL REPORT AND TRIAGE: Identifying, communicating, and triaging breach reports. Refer to Section 4.1.
2. CONTAIN: Taking immediate action to contain the breach as soon as possible to prevent any further compromise of personal information and minimise harm to affected individuals. Refer to Section 4.2.
3. ASSESS AND MITIGATE: Assessing the data breach to understand the risks associated with the data breach, and identifying and taking all appropriate actions to limit the impact of the data breach. Refer to Section 4.3.

4. NOTIFY: Notifying the NSW Privacy Commissioner and affected individuals of eligible data breaches. Refer to Section 4.4.

5. REVIEW: Reviewing and considering what actions can be taken to prevent future breaches and assessing the effectiveness of the data breach response process. Refer to Section 4.5.

4.1. INITIAL REPORT AND TRIAGE

Where possible, the person who identified the suspected data breach should try and provide the following information:

- contact name and number of persons reporting the incident,
- the type of data or information involved,
- whether the loss of the data puts any person or other data at risk,
- location of the incident,
- date and time the breach occurred,
- location of data or equipment affected,
- type and circumstances of the incident.

The Privacy Officer will undertake an initial assessment of the reported data breach, in consultation with relevant internal stakeholders. This assessment will consider:

- the type and sensitivity of information involved,
- whether the information was protected by security measures,
- the persons to whom the information was exposed,
- the risk of harm to the individuals involved and the nature of any potential harm.

Depending on the nature and severity of the breach, it may be necessary to convene a Data Breach Response Team to investigate and manage Council's response. On advice from the Privacy Officer, the General Manager will determine if a Data Breach Response Team is to be convened and select the members of the Data Breach Response Team. A member of the Data Breach Response Team may be:

- An officer or employee of Maitland City Council, or
- An officer or employee of another public sector agency acting on behalf of Maitland City Council, or
- A person acting on behalf of Maitland City Council, or a person employed by that person (e.g., an individual employed by a third party to carry out the assessment for Maitland City Council).
- To the exclusion of any person the General Manager reasonably suspects was involved in an act or omission that led to the data breach.

4.2. CONTAIN

Under section 59E(2)(a) of the PPIP Act, once becoming aware that there are reasonable grounds to suspect there may have been an eligible data breach, Council will immediately make all reasonable efforts to contain the breach as soon as possible to prevent further compromise of personal information and minimise harm to affected individuals.

'Containing' a data breach means limiting its extent, duration, or preventing it from intensifying.

What efforts are reasonable to contain a breach will depend on the circumstances and severity of the breach, including:

- The type of data breach.
- Who has access to the personal information.
- The extent to which the breached personal information is still being shared, disclosed, or lost without authorisation.

- The degree of harm that may result from continued exposure or dissemination of the records and the likelihood of such harm occurring, noting that agencies should mitigate even minor harms unless the cost, time and effort required to do so are excessively prohibitive.
- The availability and suitability of containment measures, considering their effectiveness, their impact on other individuals or agency operations, their practicality, and other relevant factors such as whether they would result in loss of evidence.

During this preliminary stage, care must be taken not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable Council to address all risks posed to affected individuals or Council.

4.3. ASSESS AND MITIGATE

After a suspected data breach is reported, an assessment must be carried out within 30 days and in an expeditious way to determine whether there are reasonable grounds to believe that the suspected data breach is in fact an eligible data breach.

Under section 59F of the PPIP Act, when assessing a data breach, the General Manager must make all reasonable attempts to mitigate the harm done by the suspected breach.

4.3.1. Assessing a data breach

The assessment of the data breach will involved:

1. Information gathering: collect all relevant information regarding the suspected breach. This may involve contacting relevant stakeholders, identifying what information was or may have been compromised, and investigating logs or other evidence from compromised systems that may be relevant to the assessment of the suspected breach.

2. Analysis: review the information collected during the previous phase to evaluate the scale, scope, and content of the suspected data breach and its potential impact on affected individuals.

3. Decision: come to a decision as to the eligibility of the suspected data breach based on the factors considered throughout the analysis. The General Manager is responsible for determining if an eligible data breach has occurred.

Council will consult the Guidelines issued by the NSW Privacy Commissioner on the assessment of data breaches.

4.3.2. Determining if a data breach is an eligible data breach

For a data breach to constitute an 'eligible data breach' under the MNDB Scheme, there are two tests to be satisfied:

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency 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.

Whether a data breach is likely to result in serious harm requires an objective assessment based on information immediately available or following reasonable inquiries or an assessment of the data breach.

Harms that can arise as the result of a data breach are context-specific and will vary based on:

- the type of personal information accessed, disclosed, or lost, and whether a combination of types of personal information might lead to increased risk,
- the level of sensitivity of the personal information accessed, disclosed, or lost,

- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach,
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm),
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance, or inconvenience.

Harm to an individual includes physical harm; economic, financial, or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in Council's position would identify as a possible outcome of the data breach.

It is important to note that breaches of personal information can result in significant harm, including people having their identify stolen or the private home addresses of vulnerable people being disclosed. As such, even a breach affecting an individual or a small number of people may have a large impact.

Council will consult the Guidelines issued by the NSW Privacy Commissioner when determining whether there has been an eligible data breach and whether the serious harm threshold has been met.

Data breach incident register

Council will establish and maintain an internal register for eligible data breaches, in accordance with section 59ZE of the PPIP Act. Each eligible data breach must be entered on the register, with the following information included for each entry where practicable:

a) who was notified of the data breach,
b) when the data breach was notified,
c) the type of data breach,
d) details of steps taken to mitigate harm done by the data breach,
e) details of the actions taken to prevent future breaches,
f) the estimated cost of the breach.

Maintaining a data breach incident register is important for record-keeping and reporting purposes, as well as to comply with any request for information from the NSW Privacy Commissioner.

The data breach incident register will be maintained by the Governance unit.

4.3.3. Mitigation strategies

The strategies we put in place to mitigate the risk of harm to affected individuals will vary depending on the type and nature of the breach, and the potential harm to individuals the breach may cause.

Notification, which enables affected individuals to take action to protect themselves, is the most common mitigation measure. However, in many cases, additional mitigation steps are appropriate.

When a data breach affects certain individuals particularly severely, it may be appropriate to provide tailored support to meet their needs, which could include counselling, enhanced security, relocation assistance, or financial compensation.

When a data breach has an impact on a wider group of individuals, it may be more appropriate to focus on more scalable support options, such as helplines for advice about the breach, or referral to specialist identity theft and cybersecurity counselling services such as ID Support NSW and IDCARE.

Other examples of mitigation measures include:

- Implementing additional security measures to limit the potential for misuse of compromised information. For example, by resetting passwords or adding additional requirements for proof of identity (POI) tests.
- Limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites. Engaging with other websites on which compromised personal information may be displayed and ask them to remove the 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 to advise caution when relying on particular identity documents for particular cohorts, or to arrange for free replacement identity documents for affected individuals. (Note that any such engagement must be consistent with the IPPs).
- Where a data breach has led to direct financial harm, offering reimbursement or compensation for other types of harm.
- Where a data breach has exposed affected individuals to serious safety risks, supporting the installation of upgraded home security or cover relocation costs (if appropriate).

4.4. NOTIFY

Agencies must notify both the NSW Privacy Commissioner and affected individuals of an eligible data breach.

When the General Manager determines that an eligible data breach has occurred, the following notification process is triggered:

1. Notify the NSW Privacy Commissioner: Once it is determined that an eligible data breach has occurred, the General Manager must immediately notify the NSW Privacy Commissioner about the breach in the approved form. Refer to Section 4.4.1.
2. Determine whether an exemption applies: If an exemption applies in relation to the eligible data breach, we may not be required to notify affected individuals. Refer to Section 4.4.2.
3. Notify affected individuals: Unless an exemption applies, we will take reasonable steps to directly notify affected individuals or their authorised representative as soon as practicable. Where we are unable to directly notify any or all affected individuals, we must issue and publicise a public notification. Refer to Section 4.4.3.
4. Provide further information to the NSW Privacy Commissioner: We may be required to provide additional information to the NSW Privacy Commissioner if we have been unable to provide complete information in our immediate notification, if we are relying on an exemption, or if we have made a public data breach notification. Refer to Section 4.4.4.

4.4.1. Notification to NSW Privacy Commissioner

If the General Manager determines that the data breach is an eligible data breach, or that there are reasonable grounds to believe that the data breach is an eligible data breach, then the General Manager must immediately notify the NSW Privacy Commissioner (s59M(1), PPIP Act).

Notification to the NSW Privacy Commissioner must be given in the approved form published by the NSW Privacy Commissioner, and must include (s59M(2), PPIP Act):

- The information that will need to be provided to individuals if no exemption applies (see section 4.4.3.4).
- The following additional information:
    - A description of the personal information that was subject to the breach.
    - Whether the General Manager is reporting on behalf of other agencies involved in the breach.
    - Whether the breach is a cyber incident and details of the cyber incident (if applicable).
    - The estimated cost of the breach to Council.
    - The total number (or estimate) of individuals:
        - affected or likely affected by the breach, and
        - notified of the breach.
    - Whether the individuals have been notified of the complaints and internal review procedures.

Data Breach Notification to the Privacy Commissioner

A follow-up notification will be provided to the NSW Privacy Commissioner, in the approved form, of any information that was not included in our initial notification (s59Q, PPIP Act).

4.4.2. Exemptions

After notifying the NSW Privacy Commissioner, we must notify affected individuals unless an exemption applies. The exemptions are:

- Where an eligible data breach affects multiple public sector agencies, and another agency has undertaken to notify individuals (s59S, PPIP Act). We will still conduct our own assessment, containment, and mitigation, and notify the NSW Privacy Commissioner.
- Where notification of the eligible data breach would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or a tribunal (s59T, PPIP Act).
- Where we have taken mitigation action that successfully prevents serious harm from occurring, so that a reasonable person would conclude that the breach is no longer likely to result in serious harm to an individual (s59U, PPIP Act).
- Where notification would be inconsistent with a secrecy provision in another Act (s59V, PPIP Act).
- Where notification would create a serious risk of harm to an individual's health or safety (s59W, PPIP Act).
- Where notification would worsen the agency's cyber security or lead to further breaches (s59X, PPIP Act).

Where we are relying on exemptions relating to health or safety or cyber security, we must provide a written notice to the NSW Privacy Commissioner advising of our reliance on the exemption and provide other specified information.

We must keep appropriate records of any assessment and decision-making process leading to reliance on an exemption.

4.4.3. Notification to affected individuals

If there is an eligible data breach and none of the exemptions apply, we must notify relevant individuals of the eligible data breach as soon as practicable.

For most people, receiving a notification that their personal information has been breached can be very stressful. In some cases, it can have a significant impact on an individual's emotional and psychological wellbeing, particularly where they are at risk or especially vulnerable.

4.4.3.1. When should we notify?

Notification to individuals must be made as soon as reasonably practicable after determining that a breach is an eligible data breach. Timely notification is important to help affected individuals affected by a breach take personal steps to limit or mitigate the risks of misuse or further exposure.

However, we also need to carefully balance speedy notification with ensuring that individuals are provided with reliable and accurate information about the breach. Most importantly, our notifications should provide recipients with an accurate sense of what risks may arise for them and what practical measures they can take to protect themselves.

For complex breaches or where significant numbers of individuals are affected, we may consider applying a triage system to notification. This might involve making notification in tranches based on the level of risk posed to the individual or the sensitivity of the information involved in the data breach.

4.4.3.2. Who must be notified?

We may elect to notify either:

1. Each individual to whom the compromised information relates, regardless of their risk of harm; or
2. Only affected individuals, meaning those individuals who are likely to suffer serious harm as a result of the compromise of personal information that relates to them. (s59N, PPIP Act)

If we are unable, or it is not reasonably practicable, to notify all relevant individuals, we must issue a public notification instead (see section 4.4.3.5).

4.4.3.3. How should we notify?

A notification should generally be made in writing, using clear and easily understood language.

Notifications will be sent to affected individuals by registered post, regular post, or email. The method chosen will depend on the type of contact information we hold.

In some instances, such as where the individual may be at imminent risk of physical violence as a result of a data breach, a notification will be by phone, followed by a written notification.

4.4.3.4. What should be included in the notification?

Section 59O of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

a) the date the breach occurred,
b) a description of the breach,
c) how the breach occurred,
d) the type of breach that occurred (*unauthorised disclosure; authorised access; loss of information*),
e) the personal information included in the breach,
f) the amount of time the personal information was disclosed for,
g) actions that have been taken or are planned to secure the information, or to control and mitigate the harm done,
h) recommendations about the steps an individual should take in response to the breach,
i) information about complaints and internal reviews of agency conduct,
j) the name of the agencies that were subject to the breach,
k) contact details for the agency subject to the breach or the nominated individual to contact about the breach.

The aim of the notification is to provide recipients with an accurate sense of what happened, what risks may arise, and what they can to protect themselves such as changing account passwords or being alert to possible scams resulting from the data breach.

4.4.3.5. Public notification

If it is not reasonably practicable to notify any or all of the individuals affected by the breach directly, Council will issue a public notification instead, in accordance with section 59N(2)(a) of the PPIP Act.

Direct notification to all affected individuals may be impossible or not reasonably practicable for a range of reasons, such as where a breach involves older records, and we do not hold (and cannot practicably obtain) current, direct contact details for some or all of the affected individuals.

We may also decide to make a public notification concurrently with direct notifications to affected individuals.

A public notification must include all the same information that would be included in a direct notification, but should exclude:

- personal information about an individual. For example, we may exclude information about specific individuals involved in the breach or breach response.
- information that would prejudice Council's functions. For example, we may omit certain details about a breach if they would expose a confidential investigation or publicise a vulnerability that still exists and can be further exploited.

If making a public notification, we must:

- Keep a public notification register on our website.
- Publish the notification on the public notification register for at least 12 months.
- Advise the NSW Privacy Commissioner of how to access the notification on the public register.

In addition to publishing the notification on their website, we must take reasonable steps to publicise the contents of the statement, to increase the likelihood that it will come to the attention of those individuals at risk of serious harm. This will be done through any appropriate channels available, such as a media release, a notice on the website homepage, a recorded message on our customer service line, direct communications with stakeholders or affected individuals who are contactable, or by paid advertising.

Public notification register

Council will maintain and publish on our website a public notification register for any public data breach notifications that we have issued, in accordance with section 59P of the PPIP Act.

A 'public data breach notification' is a notification made to the public at large rather than a direct notification to an identified individual. The MNDB Scheme provides for a public data breach notification to occur in two circumstances:

- a public notification **must** be made if we are unable, or it is not reasonably practicable, to notify any or all of the individuals affected by the breach directly (s59N(2), PPIP Act), or
- where we decide to make a public notification (s59P(1)(b), PPIP Act). This does not exempt us from the requirement to make direct notifications to affected individuals if it is reasonably practicable to do so.

The PPIP Act does not prescribe the information that must be included on the register. However, the purpose of the register is to ensure that individuals are able to access sufficient information about eligible data breaches to determine whether they may be affected by the breach and take action to protect their personal information.

Our public notification register will contain the following information:

a) the date the breach occurred,
b) a description of the breach,
c) the type of breach (*unauthorised access, unauthorised disclosure, or loss of information*),
d) how the breach occurred,
e) the type of personal information that was impacted by the breach,
f) actions taken or planned to ensure that personal information is secure or to mitigate harm, to individuals,
g) recommended steps individuals should take in response to the breach,
h) date the public notification was published,
i) where to contact for assistance or information,
j) a link to the full public notification.

Any public notification we make must be published on the public notification register and remain available for at least 12 months after the date of publication (s59P(3)(a), PPIP Act).

The public notification register will be maintained by the Governance unit.

4.4.4. Further information to NSW Privacy Commissioner

We will seek to keep the NSW Privacy Commissioner updated as the breach response progresses, and as new information comes to light.

The MNDB Scheme includes several further requirements to update the NSW Privacy Commissioner on our breach response and approach to notification:

- If any information is omitted from the immediate notification to the NSW Privacy Commissioner, we will provide an updated notification once that information becomes available, in the approved form. This will usually occur once our data breach response process has been completed and individuals have been notified of the data breach (or an exemption has been determined to apply).
- If we rely on either of the exemptions relating to health or safety or cyber security, we must additionally provide a written notice to the NSW Privacy Commissioner advising of our reliance on the exemption, whether the exemption is permanent or temporary, and if temporary, the expected time the exemption is to be relied on.
- If we publish a public data breach notification, we must advise the NSW Privacy Commissioner as soon as practicable after the notification is published of how to access the notification on the public notification register (for example, by emailing the link to the public notification register on our website) (s59P(4), PPIP Act).

4.4.5. Other reporting obligations

Depending on the circumstances of the data breach and the categories of data involved, we may need to engage with:

- Cyber Security NSW
- NSW Police Force
- Australian Federal Police
- The Australian Taxation Office
- The Australian Digital Health Authority
- The Department of Health
- The Australian Cyber Security Centre
- Foreign regulatory agencies
- Financial services providers
- Any third-party organisations or agencies whose data may be affected.

4.4.6. Collection, use and disclosure of personal information for notification purposes

We may collect, use, or disclose personal information for the purpose of confirming:

a) the accuracy of the name and contact details of an affected person or a person whose personal information has been compromised, or
b) whether that person is deceased.

Section 59R of the PPIP Act provides Council with a limited exemption to the obligation to comply with an IPP, a Health Privacy Principle, a privacy code of practice or a health privacy code of practice. The exemption only permits the collection, and disclosure of personal information between public sector agencies, and only so far as reasonably necessary for the above purposes. Additionally, the exemption is limited to the following types of personal information:

a) the name of an individual
b) the contact details of the individual
c) the date of birth of the individual
d) an identifier for the individual (for example, NSW driver license number)
e) if the individual is deceased—the date of death of the individual.

4.5. REVIEW

4.5.1. Documenting issues and remedies

Following a data breach, a post incident review will be undertaken to identify and remediate any processes or weaknesses in information security and data handling that may have contributed to the data breach to prevent future breaches, and to assess the effectiveness of the Data Breach Policy and the data breach response process.

The post incident review will be undertaken by the Privacy Officer, or the Data Breach Response Team if one is convened, in consultation with key internal and external stakeholders.

The post incident review will cover:

- A root cause analysis of the data breach.
- The effectiveness of the Data Breach Policy and data breach response process itself.
- Updates to relevant policies and procedures.
- If required, more focused reviews of particular systems, policies and procedures involved in the breach. For example,
  - If the breach exposed a large number of old and unnecessary records, a review of data retention and deletion processes.
  - If the breach involved human error in a manual process, a review of how the process might be made safer.
  - If the data breach involved a security flaw in a particular system or collection of systems, a security review and root cause analysis.
  - If the data breach involved a vendor, a review of that vendor's contractual arrangements and security practices.

A post incident report will be prepared and presented to the Executive Leadership Team and Council.

4.5.2. Review and update Data Breach Policy and Data Breach Response Plan

A review of Council's Data Breach Policy and this Plan will be undertaken after every data breach response and updated to address any opportunities for improvement that may have been identified.

5. THIRD-PARTY BREACHES

Council includes contractual terms in outsourcing arrangements that require vendors and third parties to comply with Privacy Laws, protect personal information from unauthorised access, modification, disclosure, or use, and immediately notify Council in writing if they become aware of any unauthorised access, modification, disclosure or use of personal information or privacy breach, in respect of personal information obtained under or in relation to the agreement with Council. Contracts for larger transactions (greater than $25,000) also contain a cyber security clause, requiring the vendor/third party not to expose Council to any material cybersecurity risk and immediately notify Council of any actual or suspected breach of the clause.

When dealing with a third-party breach, Council will:

- Have our Legal Counsel review relevant contracts to understand parties' rights and obligations in detail.
- Work collaboratively with the third party to understand the nature and extent of the breach. Where the affected third party is a smaller service provider, this may include stepping in to assist them with containment or other steps.
- Where the affected third party is a large supplier with contracts across multiple public sector agencies, Council will work with other affected agencies to jointly engage with the vendor on containment and remediation actions.

6. BREACHES INVOLVING MORE THAN ONE AGENCY

In the event of a data breach affecting personal information that is jointly held between Council and other agencies, Council is still required to assess the breach and if the breach is determined to be an eligible data breach, notify the NSW Privacy Commissioner, in accordance with this Plan.

However, only one of the affected agencies is required to notify affected individuals or make a public notification (if required). The PPIP Act does not specify which agency is responsible for such notification. This will be determined on a case-by-case basis. In general, the agency with the most direct relationship with the affected individuals will notify and provide direct support as required.

7. TRAINING AND AWARENESS

We will provide regular training to Council staff and contractors on the importance of safeguarding personal information, how to identify and report a suspected data breach, and the roles and responsibilities for managing data breaches.

8. TESTING AND REVIEW OF THIS PLAN

This Plan will be reviewed, tested, and updated on an annual basis.

The Privacy Officer will be responsible for reviewing and updating this Plan.

The Privacy Officer will be responsible for planning, initiating, overseeing, and reporting on the testing of the Data Breach Policy and this Plan, in consultation with relevant internal and external stakeholders.

9. PRIVACY RESOURCES

The Information and Privacy Commission NSW ('IPC') has developed a number of resources to assist public sector agencies in complying with their obligations under NSW privacy laws, including the PPIP Act and HRIP Act.

The IPC website will be regularly updated as new resources and information becomes available.

IPC Mandatory Notification of Data Breach Scheme resources