

Privacy Management Plan

2 April 2026

Policy

Contents

1. Key Information.....	4
2. Definitions	5
3. How Council manages personal and health information	5
3.1 About personal information	5
3.2 About health information	6
4. How Council collects personal and health information.....	6
4.1 Privacy Protection Notice under Section 10 of the Privacy and Personal Information Protection Act 1998 (PPIPA).....	7
4.2 Storage, access and accuracy of personal information.....	8
4.3 Use and disclosure of personal and Health information.....	8
4.4 Identity verification	9
4.5 Personal and health information use in Artificial Information systems.....	9
5. Public registers	9
5.1 Suppression of personal information	10
6. How to access and amend personal and health information	10
6.1 Limits on accessing or amending information	10
7. Data Breaches	11
7.1 What is a data breach?	11
7.2 Managing a data breach.....	11
8. Review rights and complaints	11
8.1 Internal review.....	11
8.2 Internal review process	12
8.3 The Information & Privacy Commissioner's role in internal reviews	12
8.4 External review by the NSW Civil & Administrative Tribunal.....	12
8.5 Other ways to resolve privacy concerns	12
9. Promoting privacy.....	12
10. Privacy and other legislation.....	13
10.1 The Privacy and Personal Information Protection Act.....	13
10.2 The Health Records and Information Privacy Act	15
10.3 Other relevant laws	16
10.3.1 Government Information (Public Access) Act 2009 (GIPA Act) and Government Information (Public Access) Regulation 2009.....	16
10.3.2 Independent Commission Against Corruption Act 1988	16
10.3.3 Public Interest Disclosures Act 1994 (PID Act).....	16
10.3.4 State Records Act 1998 and State Records Regulation 2010	16
10.3.5 Referrals to external agencies under other relevant legislation	17
11. Exemptions, directions and codes of practice.....	17
11.1 Privacy Code of Practice for Local Government	17
11.2 Public interest directions.....	17
12. Contact details	18
13. Roles and Responsibilities.....	18
14. Procedures	19

15. Compliance.....	19
16. Consultation	19
17. Approval and Review	19
18. Document Control	20
19. Version History.....	20
Appendix A - Key differences and interaction points.....	21
Appendix B – Privacy notification forms Disclaimer	22
Statement #1.....	22
Statement #2.....	22
Appendix C - Information Privacy Principles (IPPs)	23

1 Key Information

Privacy Management Plan

Purpose	The Privacy Management Plan explains how the Council will manage personal information in line with the Privacy and Personal Information Protection Act 1998 (PPIP Act) and health information in accordance with the Health Records and Information Privacy Act 2002 (HRIP Act). Council is required to have a Plan under s33 of the PPIP Act. This Plan also explains how to contact Council about the personal and health information it holds, how information can be accessed and amended and how privacy complaints are handled.		
Scope	Section 33(2) of the PPIP Act sets out the requirements of this Plan. This Plan must include: • Information about Council's policies and practices to ensure compliance with the PPIP Act and the HRIP Act • How staff and contractors are made aware of these policies and practices • The internal review procedures • Anything else considered relevant to the Plan in relation to privacy and the personal and health information Council holds. Any reference to staff in this document also includes reference to contractors.		
Related Documents	This document should be read in relation to: • Privacy and Personal Information Protection Act 1998 • Health Records and Information Privacy Act 2002 • Privacy Code of Practice for Local Government • Local Government Act 1993 • Government Information (Public Access) Act 2009 • Model Privacy Management Plan for Local Government Jan 2013 • Council's Code of Conduct • Council's Records Management Policy • Council's Access to Information Policy		
Compliance Requirements	• Local Government Act 1993 (NSW) • Local Government (General) Regulation 2021		
Policy Owner	Manager Governance and Risk		
Date Adopted	2/04/2026	Review Date	31/03/2029

2 Definitions

The definitions of certain terms are:

Term	Meaning
Employee	means, for the purposes of this Plan, any person working as a direct employee of the Council whether in a casual, term or permanent capacity or in the capacity of board or committee member or in the capacity of a contractor (e.g. a third-party contractor, contingent labour, consultant, work experience).
Health Information	means Personal Information that is information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided or to be provided to a person, see section 6 of the Health Records and Information Protection Act 2002.
Health Privacy Principles	means the principles set out in Schedule 1 of the HRIP Act.
HRIP Act	means the Health Records and Information Protection Act 2002 (NSW).
Information Protection Principles	means the principles set out in Division 1 of Part 2 of the PPIP Act.
Personal Information	means information or an opinion (including information or an opinion forming part of a database and whether recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, including such things as name, email address, mobile phone number or residential address. Health Information is excluded from the definition of Personal Information, except for the purposes of the MNDB Scheme. Other exclusions from Personal Information are also set out in section 4(3) of the PPIP Act.
PPIP Act	means the Privacy and Personal Information Protection Act 1998 (NSW).
Privacy Principles	means the Information Protection Principles and the Health Privacy Principles.

3 How Council manages personal and health information

3.1 About personal information

Personal information is defined in section 4 of the PPIP Act as any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained.

There are some kinds of information that are not personal information. This includes information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official.

3.2 About health information

Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act. Health information can include information about a person's physical or mental health such as a psychological report, blood test or an x-ray, and information about a person's medical appointments.

It can also include some personal information that is collected to provide a health service, such as a name and telephone number. In this section, a reference to personal information is also a reference to health information.

4 How Council collects personal and health information

Council collects personal and health information in a variety of ways to perform services and functions. Council assesses the level of personal information that is appropriate to be collected on a case-by-case basis with a view to minimizing the amount of personal and health information it collects and manages.

Personal and health information may be collected from:

- Members of the public
- NSW and Commonwealth public sector agencies
- Businesses
- Non-government organisations
- Employees
- Medical professionals

Contractors acting on Council's behalf may also collect personal information. Council includes clauses in its contracts that require contractors to comply with relevant privacy obligations.

Council has a range of functions requiring or involving the collection of personal and health information, including:

- Levying and collecting rates
- Providing services, for example, childcare, libraries and waste collection
- Consultation with the community, businesses and other stakeholders
- Assessing development and major project applications
- Recording, investigating, and managing complaints and allegations
- Site inspections and audits
- Incident management
- Enforcing regulations and legislation
- Issuing approvals, consents, licences and permits
- Providing funding grants
- Recruiting and employment
- Fitness for work

- Developing AI inputs and outputs generated or inferred by AI

Personal and health information may be collected by Council in any of the following ways:

- Incident reports
- Medical assessment reports
- Immunisation history statements
- Submissions
- Application forms (including employment)
- CCTV footage
- Public registers
- Financial transaction records
- Contracts
- Customer enquiries
- Telematics
- Waste app - video footage
- Online services
- Body cameras worn by staff
- Images, video footage and/or audio recordings from Council events
- Annual disclosure of interest declarations
- Event registrations
- Contract tracing under NSW Public Health Orders

Personal and health information may be collected electronically, in writing, over the telephone and in person. Individuals may provide Council with personal information when they make enquiries and when Council delivers services to them.

This can include names, contact details, opinions, health conditions, family relationships, housing or tenancy information, work and education details. Individuals may also provide Council with personal information about other people.

4.1 Privacy Protection Notice under Section 10 of the Privacy and Personal Information Protection Act 1998 (PPIPA)

When Council collects personal information from an individual, such as their name, address, telephone number or email address, Council must make the individual aware of:

- The purposes for which the information is being collected
- The intended recipients of the information
- Whether the supply of information is required by law or is voluntary
- Any consequences for the individual if the information (or any part of it) is not provided
- Ways the individual can access and correct the information
- The name and address of the unit that is collecting the information and the unit that is to hold the information.

To ensure Council complies with the PPIPA a Privacy Statement is included on all forms, letters and documents that collect personal information from individuals. Council's Privacy Statements appears in [Appendix B](#).

When Council gathers personal information via the telephone or other electronic means, such as a website, this information will also be provided to them.

4.2 Storage, access and accuracy of personal information

Council will ensure personal and health information is secure (electronically and physically) and it will only keep it for as long as it is appropriate. Personal information is secured by:

- Monitoring network traffic using industry standard practice, processes, procedures and tools.
- Undertake penetration testing annually.
- Complying with State Records Act in relation to safe custody, preservation, accuracy, maintenance and disposal of state records; and
- Ensuring staff compliance with the Computer Resource Usage Policy.

Electronic information is stored on secure information systems. Networks will be secure and require individual login. New systems for storing personal and /or health information are assessed for compliance with the PPIP Act and HRIP Act.

The following applies to information Council holds:

- Only Council staff can access personal information
- Staff will make every effort to ensure personal information is accurate before using it
- Staff will use personal information only for the purpose for which it was collected; and
- Staff will not disclose personal information about a person to anyone without the consent of the person, or if legally required or permitted to disclose information.

4.3 Use and disclosure of personal and Health information

Council will use your personal and health information for the purpose for which it was collected. Council may use it as is necessary for the exercise of other council functions where it is satisfied that personal and health information is reasonably necessary for the exercise of such functions (i.e. to deliver services, conduct research, log requests and provide advice to our customers)

Council does not disclose personal or health information without consent, unless the disclosure is:

- For a purpose directly related to the reason Council collected it, and Council has no reason to believe the individual would object,
- Necessary to prevent or lessen a serious and imminent threat to someone's life or health, or
- Permitted under the PPIP Act, the HRIP Act or other legislation.

Council will not disclose personal information relating to a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities without consent, unless such disclosure is necessary to prevent or lessen a serious and imminent threat to life or health.

Council will allow people to remain anonymous where it is lawful and practicable. For example, where possible our online surveys and other community engagement initiatives allow for feedback to be given anonymously.

4.4 Identity verification

Individuals may provide Council with documents to verify their identity, for example a driver's licence when they make an application for a parking permit, busking permit or a GIPA application.

Where possible Council will not retain copies of personal identity documents. State Records NSW provides authorisation to the effect that copies of records used to verify the identity of a customer or collected as part of a recruitment process can be retained until verification or validation process has been completed and then destroyed. This approach is supported by organisational procedures and record management reviews.

4.5 Personal and health information use in Artificial Information systems

Council will consider how the AI use case complies with PPIP Act and the HRIP Act. Both acts apply to personal and health information inputted into an AI system, as well as the output generated or inferred by an AI system that contains such information.

The management of personal and health information in AI systems is similar to other uses outlined in the policy. In general:

- Council establishing clear processes for verification of AI outputs containing personal and health information and adding transparent information about its use of AI in its privacy policy.
- AI inputs or outputs generated or inferred by AI, which contain personal information, must be reasonably necessary for, or directly related to, Council's functions or activities. Additionally, if the AI input or output comprises sensitive personal information, the individual must consent unless another exception applies. Collection must occur by fair and lawful means.
- Council will notify individuals of AI-related purposes for which their personal and health information is being collected and any proposed use of AI to generate outputs which contain personal information.
- Council will only input an individual's personal information into an AI system, or use or disclose AI outputs which contain personal and health information, for the primary purpose for which the agency collected the information, unless they have consent or another exception applies – for example, if Council can establish a related secondary use would be reasonably expected by the individual.
- Council will take reasonable steps to ensure personal and health information collected, used and disclosed by the AI system is accurate, up-to-date, complete and relevant.
- Council will take reasonable steps to protect personal and health information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

5 Public registers

The PPIP Act governs how Council should manage personal information contained in public registers. Under the PPIP Act a public register is a register of personal information that is required by law to be made, or is made, publicly available or open to public inspection.

Enquiries about public registers can be made via Council's website.

Part 6 of the PPIP Act prevents Council staff from accessing personal information held on public registers, unless the information is to be used for a purpose relating to the purpose of the register.

Council's public registers include:

- Land register (LG Act s53)
- Register of Approvals (LG Act s113)
- Register of Political Donations Declarations (LG Act 328A)
- Planning Decision Register (LG Act 375A)
- Register of Disclosures of Interests by Councillors & Designated Persons (LG Act s440 and GIPA Act s6)
- Rates Record (LG Act s602)
- Planning Decision Register (EP&A Act s100)
- Register of Political Donations and Gifts (EP&A Act s147)
- Record of building certificates (EP&A Act s149a)
- Contributions Register (EP&A Reg cl34)
- Public record of licences (POEO Act s308)
- Record of impounding (Impounding Act s30-31)

5.1 Suppression of personal information

Any person whose personal information is recorded in a public register has the right to request that their personal details be suppressed. Council will comply with the request if it is satisfied the person's safety or wellbeing would be affected by not suppressing the information.

Applications to suppress personal details from a public register should be made in writing to the General Manager.

Council also has obligations under GIPA Act to make open access information publicly available (including on its website) unless there is an overriding public interest against disclosure of the information. Council must facilitate public access to open access information contained in a record by deleting matter (e.g. personal information) from a copy of the record to be made publicly available if inclusion of the matter would otherwise result in there being an overriding public interest against disclosure of the record and it is practicable to delete the matter.

6 How to access and amend personal and health information

The PPIP Act and the HRIP Act give people the right to access and amend their own information. Members of the public wishing to access or amend personal and health information Council holds about them should contact Council's Customer Service Centre.

Council does not charge a fee to access and amend personal and health information.

6.1 Limits on accessing or amending information

Council is prohibited from providing one person access to another person's personal and health information. However:

- Under section 26 of the PPIP Act, a person can give Council consent to disclose their personal information to someone that would not normally have access to it
- Under sections 7 and 8 of the HRIP Act, an “authorised person” can act on behalf of someone else
- Council may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual, to find a missing person or for compassionate reasons.

7 Data Breaches

7.1 What is a data breach?

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to Council's physical or electronic information or data, such as:

- Accidental loss or theft of information or equipment on which such information is stored.
- Unauthorised use, access to or modification of data or information systems to gain unauthorised access or make unauthorised changes to data or information.
- Accidental or unauthorised disclosure of personal information (e.g., email containing personal information sent to the incorrect recipient).
- Personal information published or posted on Council's website without consent.
- Access to data by an authorised user for unauthorised reasons (e.g., an employee looking up information in a system for personal reasons in breach of the Code of Conduct).
- Accidental disclosure of user login details through phishing.
- Malware infection; or
- Disruption to or denial of IT services.

7.2 Managing a data breach

Council's separate Data Breach Policy sets out Council's procedures for managing a data breach, including the assessment and notification requirements for the Mandatory Notification of Data Breach Scheme under PIPPA.

In the event of a data breach, Council will:

- Follow the guidance issued by the Information & Privacy Commission NSW (IPC) relating to the Voluntary Reporting Scheme; and
- If the breach relates to Tax File Number information, following the protocols of the Office of the Australian Information Commissioner (OAIC) relating to Notifiable Data Breaches.

8 Review rights and complaints

8.1 Internal review

Individuals have the right to seek an internal review under Part 5 of the PPIP Act if they think that Council has breached the PPIP Act or HRIP Act relating to their own personal and health information.

Individuals cannot seek an internal review for a breach of someone else's privacy, unless they are authorised representatives of the other person.

8.2 Internal review process

Applications for an internal review must be made within six months from the date when the applicant first became aware of the breach.

Applications must be made in writing and addressed to Council's Public Officer.

The Public Officer will conduct the internal review unless the internal review is about the conduct of the Public Officer.

In this case the General Manager will appoint another person to conduct the internal review.

Council will:

- Acknowledge receipt of an internal review within 5 working days.
- Complete an internal review within 60 calendar days.

Council's Public Officer will inform the applicant of the progress of the internal review and will respond in writing within 14 calendar days of determining the internal review.

If an applicant is not notified of the outcome of an internal review within 60 days, the applicant may seek an external review.

8.3 The Information & Privacy Commissioner's role in internal reviews

Council will notify the Information & Privacy Commissioner (IPC) of internal reviews. The Privacy Commissioner is entitled to make submissions to Council regarding internal reviews.

8.4 External review by the NSW Civil & Administrative Tribunal

An applicant may seek an external review by the NSW Civil & Administrative Tribunal (NCAT).

To seek an external review, an application must be made to the NCAT within 28 days from the date of the internal review determination.

8.5 Other ways to resolve privacy concerns

Council encourages the informal resolution of privacy issues before undertaking the review process. Issues can be raised informally with Council by telephone - request to speak to the Public Officer.

9 Promoting privacy

Council reinforces compliance with the PPIP Act and HRIP Act and will:

- Endorse this Plan and make it publicly available on its website.
- Providing hard copies of the Plan to members of the public free of charge upon request.
- translating the Plan into other languages and alternative formats upon request

- informing people about the Plan when responding to enquiries about personal and health information.
- provide a copy of this Plan to relevant oversight bodies such as the Audit Risk & Improvement Committee.
- Report on internal reviews to the Office of the Information and Privacy Commission; and
- identify privacy issues when implementing new systems, services and processes.

Council will ensure that its staff are aware of and understand this Plan and how it applies to the work they do. Council will promote awareness of privacy obligations among staff by:

- Publishing Council's Privacy Management Plan and privacy-related policies on Council's intranet and website.
- Publishing information about privacy on Council's intranet.
- Communicating regularly with staff about privacy.
- Ensuring Council policies comply with privacy legislation.
- Including information about the Privacy Management Plan induction packs.
- Offering training and advice to staff.

10 Privacy and other legislation

This section contains a general summary of how Council must manage personal and health information under the Privacy and Personal Information Protection Act 1998 (PPIP Act), the Health Records and Information Privacy Act 2002 (HRIP Act) and other relevant laws.

10.1 The Privacy and Personal Information Protection Act

The Privacy and Personal Information Protection Act set out how Council must manage personal information.

What is personal information?

Personal information is defined in section 4 of the PPIP Act as any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained.

What is not personal information?

There are some kinds of information that are not personal information, these include:

- Information about someone who has been dead for more than 30 years.
- Information about someone that is contained in a publicly available publication.
- Information or an opinion about a person's suitability for employment as a public sector official.

Information protection principles (IPPs) Part 2, Division 1 of the PPIP Act contains 12 IPPs Council must comply with. These are set out in [Appendix C](#).

How will personal information be collected?

Council will:

- Collect personal information only for a lawful purpose that is directly related to Council's functions and activities.

- Collect personal information directly from the person concerned.
- Inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. Also, how the personal information can be accessed and amended and any possible consequences of not providing personal information.
- Ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into people's personal affairs.

Storage

Council will ensure personal information is secure and it will only keep it for as long as appropriate. Personal information will be secured by:

- Monitoring network traffic using industry standard practice, processes, procedures and tools.
- Undertake penetration testing annually.
- Complying with State Records Act in relation to safe custody, preservation, accuracy, maintenance and disposal of state records; and
- Ensuring staff compliance with the Computer Resource Usage Policy.

Access and accuracy

Council will:

- Be transparent about the personal information it holds, why it is used and about the right to access and amend it.
- Allow people to access their own personal information without unreasonable delay or expense.
- Allow people to update, correct or amend their personal information where it is necessary; and
- Endeavour to ensure that personal information is relevant and accurate before using it.

Use

- Council will only use personal information for the purpose it was collected for unless it has consent for its use for another purpose.

Disclosure

Council:

- Will not disclose personal information without consent, unless disclosure is permitted under the PPIPA or other legislation; and
- Will not disclose sensitive personal information without consent, e.g. ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

Offences

Offences can be found in s62-68 of the PPIP Act. It is an offence for Council to:

- Intentionally disclose or use personal information for an unauthorised purpose.
- Offer to supply personal information that has been disclosed unlawfully; and
- Hinder the Privacy Commissioner or their staff from doing their job.

10.2 The Health Records and Information Privacy Act

The HRIP Act sets out how Council must manage health information. About health information Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act.

Health information can include information about a person's physical or mental health such as a psychological report, blood test or an x-ray, and information about a person's medical appointments.

It can also include some personal information that is collected to provide a health service, such as a name and telephone number. Health privacy principles (HPPs) Schedule 1 of the HRIP Act contains 15 HPPs that Council must comply with.

Collection

Council will:

- Collect health information only for a lawful purpose that is directly related to Council's functions and activities.
- Ensure that health information is relevant, accurate, is not excessive and does not unreasonably intrude into people's personal affairs.
- Collect health information directly from the person concerned.
- Inform people why their health information is being collected, what it will be used for, and to whom it will be disclosed; and
- How it can be accessed and amended and any possible consequences not providing health information.

Storage

Council will:

- Store health information securely, keep it no longer than necessary and destroy it appropriately. Health information will be protected from unauthorised access, use or disclosure.

Access and accuracy

Council will:

- Be transparent about the health information it holds, why it is used and about the right to access and amend it.
- Allow people to access their own health information without unreasonable delay or expense.
- Allow people to update, correct or amend their health information where necessary; and
- Ensure that health information is relevant and accurate before using it.

Use

- Council will only use health information for the purpose it was collected for unless it has consent for its use for another purpose.

Disclosure

- Council will not disclose personal information without consent, unless disclosure is permitted under the HRIPA or other legislation, Identifiers and anonymity.
- May use unique identifiers for health information; and
- Allow people to remain anonymous where it is lawful and practicable.

Transfers and linkage

Council:

- Does not usually transfer health information outside of NSW; and
- Does not currently use a health records linkage system.

Offences

Offences can be found in s68-70 of the HRIP Act. It is an offence for Council to:

- Intentionally disclose or use health information codes for an unauthorised purpose; and
- Offer to supply health information that has been disclosed unlawfully.

10.3 Other relevant laws

This section contains information about other relevant legislation.

10.3.1 Government Information (Public Access) Act 2009 (GIPA Act) and Government Information (Public Access) Regulation 2009

Under this Act and Regulation people can apply for access to information held by Council. This information may include personal or health information.

The Plan is publicly available as open access information under the Government Information and Public Access Act (GIPA Act).

See [Appendix A](#) for a comparison between the GIPA Act and the PPIP Act.

10.3.2 Independent Commission Against Corruption Act 1988

Under this Act Council must provide information to the Independent Commission Against Corruption about allegations of fraud and corruption that may contain personal information.

10.3.3 Public Interest Disclosures Act 1994 (PID Act)

Under the PID Act people working for a NSW public sector agency can make a public interest disclosure to Council. The PID Act requires that information that might identify or tend to identify a person who has made a public interest disclosure should be protected.

10.3.4 State Records Act 1998 and State Records Regulation 2010

This Act and Regulation authorise the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.

10.3.5 Referrals to external agencies under other relevant legislation

Under the Ombudsman Act, the Independent Commission Against Corruption Act, and the Crimes Act Council can provide information to the:

- NSW Ombudsman.
- Independent Commission Against Corruption; and
- NSW Police.

11 Exemptions, directions and codes of practice

Exemptions to the Information Protection Principles (IPPs) Part 2, Division 3 of the PPIP Act contains exemptions that may permit Council not to comply with IPPs in certain situations.

These include the following:

- Council is not required to comply with IPPs 2-3, 6-8, or 10-12 if lawfully authorised or required not to do so.
- Council is not required to comply with IPP 2 if the information concerned is collected in relation to court or tribunal proceedings.

Exemptions to the Health Privacy Principles (HPPs)

Exemptions are located mainly in Schedule 1 to the HRIP Act and may permit Council not to comply with HPPs in certain situations. For example, Council is not required to comply with HPPs 4-8, and 10 if lawfully authorised or required not to do so.

11.1 Privacy Code of Practice for Local Government

Under the Privacy Code of Practice for Local Government where it is reasonably necessary, Council may indirectly collect and use personal information to confer an award, prize, or similar form of personal recognition on the person about whom the information relates.

The Privacy Code of Practice for Local Government also permits Council to use personal information for a purpose other than the purpose for which it was collected where the use is in pursuance of Council's lawful and proper functions and the personal information is reasonably necessary for the exercise of those functions. In general, Council does not use personal information for a purpose other than which it was collected without the consent of the individual.

11.2 Public interest directions

Under section 41 of the PPIP Act, the Privacy Commissioner has made Public Interest Directions to waive or modify the requirement for a public sector agency to comply with an IPP.

The following public interest directions may permit Council:

- to be exempt from IPPs 2-3, 6-8, 10-12 in relation to the conduct of investigations
- to be exempt from the IPPs when transferring enquiries to another NSW public sector agency

- to disclose personal information collected for research purposes.

12 Contact details

Further information about Council's Privacy Management Plan, or the personal and health information Council holds can be obtained by:

Privacy Contact Officer - Bayside Council:

Telephone: 1300 581 299
 Email: governance@bayside.nsw.gov.au
 Address: 444-446 Princes Highway Rockdale NSW 2216
 Website: www.bayside.nsw.gov.au

The Office of the Information and Privacy Commissioner:

Telephone: 1800 472 679
 Email: ipcinfo@ipc.nsw.gov.au
 Address: Level 15, McKell Building,
 2-24 Rawson Place, Haymarket NSW 2000
 Website: www.ipc.nsw.gov.au

NSW Civil and Administrative Tribunal:

Telephone: 1300 006 228
 Email: aeod@ncat.nsw.gov.au
 Address: Level 10 John Maddison Tower,
 86-90 Goulburn Street Sydney NSW 2000
 Website: www.ncat.nsw.gov.au

13 Roles and Responsibilities

General Manager

The General Manager is responsible for this Privacy Management Plan overall and the provision of appropriate resources and procedures to enable its implementation.

Privacy Contact Officer

The Privacy Contact Officer is Council's Public Officer.

The Privacy Contact Officer is responsible for the promulgation, implementation and maintenance of this Plan and coordination of privacy management issues within Council generally. The Officer:

- Receives advice and updated information from the Office of the Privacy Commissioner NSW about the implementation of the PPIP Act and the HRIP Act.
- Acts as a main liaison with Office of the Privacy Commissioner NSW for all matters related to privacy and personal information.
- Acts as a focal point within Council for all matters related to privacy and personal information, including related induction of and awareness for Council officials; and
- Acts as a first point of contact for members of the public for all matters related to privacy and personal information.

Council officials

Councillors, employees, committee members and other officials are to be aware of the requirements of this Plan. Council officials are not to divulge personal information, and Council information generally, unless permitted by this Plan or Council's Access to Information Policy and associated guidelines. Certain requests, as detailed in this Plan, are to be referred to a particular officer to be dealt with.

14 Procedures

The General Manager may approve Procedures, which outline administrative arrangements, to support the Privacy Management Plan. Such procedures would include:

- Forms
- Statements
- Detailed responsibilities.

15 Compliance

Compliance with this Plan is mandatory. A breach of this Plan may be dealt with in accordance with Council's Code of Conduct.

16 Consultation

Internal consultation is undertaken with key internal stakeholders to ensure it reflects operational requirements:

- Customer Experience – engaged to ensure that the Plan aligns with Council's overall information management framework, including data breaches and reporting to external stakeholders.
- Information Technology – engaged regarding the secure storage, retrieval and destruction of personal and health information.

17 Approval and Review

Approval and Review	
Date Adopted	2/04/2026
Approver	General Manager
Owner	Manager Governance and Risk
Endorser	Executive Committee
Review period	3 years
Review Date	31/03/2029
Date to commence next review	1/07/2028

Class of document	Administrative Policy
Published	Council Website and Intranet
Unsubstantial administrative changes	Director City Performance or Manager Governance & Risk to approve non-significant and/or minor editorial amendments that do not change the substance of this Policy

18 Document Control

Content Manager			
Policy reference (PP)	PP16/6	Bayside Policy Register folder reference	F16/951
Word document reference	16/127097	Word document folder reference	F13/37.002
Evidence of approval		BP26/854	

19 Version History

Version	Date Adopted	Approved By	Author	Comment
1.0	09/11/2016	N/A	Liz Rog	New document
2.0	22/11/2023 (Council)	Executive Committee	Coordinator Governance	Review and update in light of new Data Breach Policy.
3.0	2/04/2026	Executive Committee	Lead Governance (Acting)	Review of policy and inclusion of AI use principles.
3.1	8/05/2026	Manager Governance and Risk	Lead Governance (Acting)	Conversion of V3 into the new policy template.

20 Appendices

20.1 Key differences and interaction points

Feature	GIPA Act	PPIP Act
Primary Purpose	To provide for public access to government information	To protect the privacy of individuals in NSW public sector agencies
Access to Personal Information	Allows access to personal information held by government agencies, but with its own exceptions	Regulates how agencies collect, use, and disclose personal information
Disclosure of Personal Information	Can mandate disclosure of personal information if the public interest in doing so outweighs the public interest in withholding it	Generally, prohibits disclosure unless an exception applies (e.g., for a lawful purpose related to the collection)
Health Information	Includes health information in its definition of personal information	Explicitly excludes health information from its definition of personal information, which is covered by the Health Records and Information Privacy Act 2002
Overlap and Precedence	The GIPA Act is not limited by the PPIP Act. This means that even if the PPIP Act prohibits disclosure, an agency can still release the information if the GIPA Act's public interest test is met	The PPIP Act sets out rules for agencies but acknowledges that the GIPA Act may require disclosure of personal information in some circumstances
Example of interaction	A government agency receives a GIPA application for an employee's performance review. While the PPIP Act would likely prohibit this disclosure, the GIPA Act's public interest test might require the agency to release the information if the public interest in disclosure (e.g., for transparency) is greater than the privacy concerns.	An agency cannot collect personal information for a purpose not related to its function under the PPIP Act. However, if a request is made under GIPA for information that was collected for an unrelated purpose, the agency may still be required to release it if the public interest test is met

20.2 Privacy notification forms Disclaimer

Statement #1

Bayside Council respects your privacy. Any personal information we collect from you will be handled in accordance with the Privacy & Personal Information Protection Act 1998 (PPIPA) and our Privacy Management Plan. Download a copy of our Privacy Management Plan.

Statement #2

Bayside Council respects your privacy and is committed to protecting your personal information in accordance with the Privacy and Personal Information Protection Act 1998 (PIPPA).

Council collects personal information that you voluntarily choose to provide under the and only used. However, if you cannot or do not wish to provide the information requested, Council may be limited in its ability to deal with your application/request.

Access to this information is restricted to Council officers and other Council-authorized people. Council will not share your information with other government agencies or organisations without your permission, unless it is required by law.

You may make an application to access, or to amend, your personal information held by Council. Such applications are considered by Council under the PPIPA.

20.3 Information Privacy Principles (IPPs)

#	IPP	Explanation
1	Lawful	An agency must only collect personal information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.
2	Direct	An agency must only collect personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.
3	Open	An agency must inform you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.
4	Relevant	An agency must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.
5	Secure	An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.
6	Transparent	An agency must provide you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.
7	Accessible	An agency must allow you to access your personal information without excessive delay or expense. An agency must allow you to update, correct or amend your personal information where necessary.
8	Correct	An agency must ensure that your personal information is relevant, accurate, up to date and complete before using it.
9	Accurate	An agency can only use your personal information for the purpose for which it was collected unless you have given consent, or the use is directly related to a purpose that you would expect, or to prevent or lessen a serious or imminent threat to any person's health or safety.
10	Limited	An agency can only disclose information in limited circumstances if you have consented or if you were told at the time they collected it that they would do so.
11	Restricted	An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.
12	Safeguarded	An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.



Bayside Council
Serving Our Community

Contact Us



Website:
www.bayside.nsw.gov.au



Email:
council@bayside.nsw.gov.au



Phone:
1300 581 299 or +61 2 9652 1666



Visit our Customer Service Centres
Monday to Friday 8:30am – 4.30pm
Rockdale Library, 444-446 Princes Highway, Rockdale
Westfield Eastgardens, 152 Bunnerong Road, Eastgardens



Telephone Interpreter Services - 131 450
بخدمه الترجمة الهاتفية 電話傳譯服務處

Τηλεφωνικές Υπηρεσίες Διερμηνέων
Служба за преведување по телефон