NAMBUCCA VALLEY COUNCIL

DRAFT - PRIVACY MANAGEMENT PLAN
POLICY No. CS 06

Our Vision

Nambucca Valley ~ Living at its best

Our Mission Statement

'The Nambucca Valley will value and protect its natural environment, maintain its assets and infrastructure and develop opportunities for its people.'

Contents

1.0 Purpose

The purpose of this Privacy Management Plan (PMP) is to explain how Nambucca Valley Council (Council) manages personal and health information in accordance with NSW Privacy Laws.

2.0 Related legislation/Policies

Mandatory Notification of Data Breach (MNDB) Scheme
Privacy and Personal Information Protection Act 1988 (NSW) (PPOP Act)
Health Records and Information Privacy Act 2002 (NSW) **(***HRIP Act***)**
Government Information (Public Access) Act 2009 (NSW) (GIPA Act)
CS 07 – Data Breach Policy
CS 24 - ICT Change Management Policy
CS 25 - ICT Incident Management Policy
CS 28 - Information Security and Management Policy
ICT Strategy 2022-2026

3.0 Definitions

Term	Meaning
Council	Nambucca Valley Council
DA	Development Application
DBP	Data Breach Policy
GIPA Act	*Government Information (Public Access) Act 2009* (NSW)
HPP	Health Privacy Principle
HRIP Act	*Health Records and Information Privacy Act 2002* (NSW)
IPC	Information and Privacy Commission
IPP	Information Protection Principle
LG Act	*Local Government Act 1993* (NSW)
MNDB	Mandatory Notification of Data Breach Scheme
NCAT	New South Wales Civil and Administrative Tribunal
PMP or this Plan	Privacy Management Plan
PPIP Act	*Privacy and Personal Information Protection Act 1998* (NSW)
Regulation	*Privacy and Personal Information Protection Regulation 2019* (NSW)
s	Section, when used before a number in reference to a section of an Act.
Privacy Code	Privacy Code of Practice for Local Government

4.0 Outcomes

Council is committed to embedding privacy best practice into all business practices and decision making. Council recognises that considering the impact on privacy of any new service, initiative or information system prior to design and implementation is key to this commitment.

Further, Council acknowledges and respects the right of every individual whose personal or private information is collected or held by Council, to have such information used only for the purpose that it is provided for, and to be managed in a manner that ensures confidentiality and privacy.

Whilst the main objective of this Plan is to enshrine best practice, the Plan also aims to ensure Council's compliance with:

- The *Privacy and Personal Information Protection Act 1998* (NSW) (*PPIP Act*); and
- The *Health Records and Information Privacy Act 2002* (NSW) **(***HRIP Act***)**;

Council is required to have a PMP under section (s) 33 of the *PPIP Act* which must include:

- Information about how Council develops policies and practices in line with the state's information and privacy legislation;
- How Council disseminates these policies and practices within the organisation and trains its staff in their use;
- Council's internal review procedures; and
- Anything else Council considers relevant to the Plan in relation to privacy and the personal and health information it holds.

This Plan also explains who you should contact if you have any questions about the information collected and retained by the Council, how to access and amend your stored information and what to do if Council may have breached the *PPIP Act* or *HRIP Act*.

5.0 Roles and Responsibilities

5.1 Privacy Contact Officer

Council's Privacy Contact officer is the Director Corporate Services who may be contacted via:

Email: council@nambucca.nsw.gov.au Telephone: 02 6568 2555

The role of the Privacy Contact Officer is:

- To receive advice and updated information from the Information and Privacy Commission (IPC) about the implementation of the *PPIP Act* and the *HRIP Act*;
- To act as a first point of contact/liaison with the IPC for all matters related to privacy and personal information;
- To act as a focal point within Council for all matters related to privacy and personal information including providing advice to staff who are unsure about privacy matters; and
- To act as a first point of contact for members of the public for all matters related to privacy and personal information.

The Privacy Contact Officer will be involved in the following tasks:

- Disseminating information on privacy issues within Council;

- Co-ordinating the steps to be taken by Council to implement the *PPIP Act* and the *HRIP Act*, including:

    - Privacy Management Plans;
    - Privacy Notifications (s 10); and
    - Privacy training for staff.

- Assessing complaints lodged within Council and making recommendations about whether it is about personal information under the *PPIP Act* and/or health information under the *HRIP Act*;

- Ensuring that all complaints about privacy breaches and/or internal reviews are dealt with in the proper manner; and

- Reviewing the Plan.

5.2 General Manager

The General Manager has the responsibility for appointing an appropriate officer as Council's Privacy Contact Officer to manage the day-to-day activities in relation to the appropriate collections, use and storage of personal and private information of customers and ratepayers.

5.3 Managers

Managers are responsible for ensuring their division adheres to the requirements of this Plan and providing guidance in respect of the importance of protecting the privacy and the personal information of customers and ratepayers collected and held by Council.

Managers should ensure that the privacy impacts of any new project or system development/implementation are thoroughly considered prior to implementation to allow issues of concern or risk to be addressed early in the process. Managers are to ensure that any adopted Privacy Impact Assessment process or procedure is followed whenever personal or health information will be collected, stored, used or disclosed in a project.

5.4 Staff

Staff shall adhere to the requirements of this Plan and be cognisant of the significant impact that can occur to individuals if their privacy is breached in any way or their personal information is not handled in accordance with this Plan and relevant legislation.

Staff should only access the personal information of a customer or ratepayer if it is a direct requirement of their role and should never release personal or private information to another person without prior approval by their supervisor. If any doubt exists in relation to any privacy issue, including appropriateness of collecting, using or sharing personal and private information than staff should contact the Privacy Contact Officer immediately for direction.

6.0 Policy Statement

Nambucca Valley Council acknowledges and respects the right of every individual whose personal or private information is collected or held by Council, to have such information used only for the purpose that it is provided for, and to be managed in a manner that ensures confidentiality and privacy.

The *PPIP Act* provides for the protection of personal information by means of twelve Information Protection Principles (IPPs). Those principles are listed below:

- Principle 1 - Collection of personal information for lawful purposes;
- Principle 2 - Collection of personal information directly from individual;
- Principle 3 - Requirements when collecting personal information;
- Principle 4 - Other requirements relating to collection of personal information;
- Principle 5 - Retention and security of personal information;
- Principle 6 - Information about personal information held by agencies;
- Principle 7 - Access to personal information held by agencies;
- Principle 8 - Alteration of personal information;
- Principle 9 - Agency must check accuracy of personal information before use;
- Principle 10 - Limits on use of personal information;
- Principle 11 - Limits on disclosure of personal information; and
- Principle 12 - Special restrictions on disclosure of personal information.

Those principles are *modified* by the Privacy Code of Practice for Local Government (the Privacy Code) made by the Attorney General.

The Privacy Code has been developed to enable Local Government to fulfil its statutory duties and functions under the *Local Government Act 1993* (NSW) (the *LG Act*) in a manner that seeks to comply with the *PPIP Act*.

This Plan outlines how Nambucca Valley Council will incorporate the twelve IPPs into its everyday functions. This Plan should be read in conjunction with the Privacy Code.

Nothing in this Plan is to:

- Affect any matter of interpretation of the Codes or the IPPs and the Health Privacy Principles as they apply to Council;
- Affect any obligation at law cast upon Council by way of representation or holding out in any manner whatsoever; or
- Create, extend or lessen any obligation at law which Council may have.

This Plan is designed to introduce policies and procedures to maximise compliance with the *PPIP Act* and the *HRIP Act*.

Where Council has the benefit of an exemption, it will nevertheless describe procedures for compliance in this Plan. By doing so, it is not to be bound in a manner other than that prescribed by the Codes.

Council collects, stores and uses a broad range of information. A significant part of that information is personal information. This Plan applies to that part of Council's information that is personal information.

It may mean, in practice that any information that is not personal information will receive treatment of a higher standard; namely treatment accorded to personal information where the information cannot be meaningfully or practicably separated.

6.1 What is Personal and Health Information

6.2 Personal information

Personal information is defined in s 4 of the *PPIP Act* as information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This information can be on a database and does not necessarily have to be recorded in a material form.

6.3 What is not personal information under the PPIP Act?

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; and
- Information or an opinion about a person's suitability for employment as a public sector official.

The *Privacy and Personal Information Protection Regulation 2019* (the *Regulation*) also lists other information that is not personal information, such as information about someone that is contained in:

- A document in a library, art gallery or museum;
- State records under the control of the NSW State Archives and Records; and
- Public archives (within the meaning of the *Copyright Act 1968* (Cth)).

6.4 Health Information

Health information is a more specific type of personal information and is defined in s 6 of the *HRIP Act*. Health information can include 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 to a person.

Health information can include, for example, a psychological report, blood test or an x- ray, results from drug and alcohol tests, 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.

6.5 Why does Council collect Personal and Health Information?

Council collects personal information in a variety of ways to efficiently perform its services and functions. Council assesses the level of personal information that is appropriate to be collected in relation to each function undertaken with a view to minimise the amount of such 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; and
- 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 involving the collection of personal/health information, including:

- Levying and collecting rates;
- Providing services, for example, 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 grant funding;
- Maintaining the non-residential register of electoral information; and
- Employment practices, including assessing fitness for work.

6.6 How does Council collect Personal and Health Information

Council collects personal information in a variety of ways including:

- Incident reports;
- Medical assessment reports;
- Submissions;
- Application forms;
- CCTV footage;
- Financial transaction records;
- Contracts;
- Customer enquiries and correspondence;
- Telematics;
- Web services and smart devices (the Internet of Things); and
- Contact tracing under NSW Public Health Orders.

6.7 Unsolicited information

Unsolicited information is personal, or health information provided to Council in circumstances where Council has not asked for or required the information to be provided. Such information is not deemed to have been collected by Council but the access, storage, use and disclosure IPPs in this Plan will apply to any such information, whilst Council continues to hold this information.

Personal information contained in petitions received in response to a call for submissions or unsolicited petitions tabled at Council meetings will be treated the same as any other submission and may be made available for release to the public.

Personal or health information disclosed publicly and recorded for the purposes of webcasting at Council Meetings is not deemed to have been collected by Council. Retention and Use Principles of this information will apply to such information in Council's possession; however, Disclosure Principles will not apply as the information was voluntarily disclosed with the prior knowledge that it would be recorded, broadcast via the internet to the public and made available by Council for public viewing.

6.8 Privacy Protection Notice

Under s 10 of the *PPIP Act*, when Council collects personal information from an individual, such as their name, address, telephone number or email address, Council must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual is made aware of:

- The purposes for which the information is being collected;
- The intended recipients of the information;
- Whether the supply of the information is required by law or is voluntary;
- Any consequences for the individual if the information (or any part of it) is not provided; and
- The ways in which the individual can access and correct the information.

Where possible, individuals providing personal information will be given the opportunity to consent to the terms of the provision of the information via a Privacy Protection Notice. Council staff are encouraged to consult with the Privacy Contact Officer to ensure that each collection of personal information, and any accompanying Privacy Protection Notice is appropriate and complies with Council's privacy requirements.

6.9 Personal or Health Information held by Council

Nambucca Valley Council holds personal information concerning Councillors, such as:

- Personal contact information;
- Complaints and disciplinary matters;
- Pecuniary interest returns; and
- Entitlements to fees, expenses and facilities.

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

- Rates records; and
- Development Applications (DA's) and objections; and
- Various types of health information.

Nambucca Valley Council holds personal information concerning its employees, volunteers and contractors, such as:

- Recruitment material;
- Leave and payroll data;
- Personal contact information;
- Performance management plans;
- Disciplinary matters;
- Pecuniary interest returns;
- Wage and salary entitlements; and Health information (such as medical certificates and workers compensation claims).

6.10 Applications for suppression in relation to general information (not public registers)

Under s 739 of the *LG Act* a person can make an application to suppress certain material that is available for public inspection in circumstances where the material discloses or would disclose the person's place of living if the person considers that the disclosure would place the personal safety of the person or their family at risk.

Section 739 of the *LG Act* relates to publicly available material other than public registers. As such, it limits disclosure in those circumstances where an application for suppression is successful. An application for suppression must be verified by statutory declaration and otherwise meet the requirements of s 739. When in doubt, Council will err in favour of suppression.

6.11 How Council manages Personal and Health Information

As outlined elsewhere in this Plan, Council collects and manages information from a multitude of sources and will always do so in accordance with the *PPIP Act*. Council also endeavours to make as much information available, to individuals whose information it collects/holds, at the time of collection. Additional information is detailed below for services / functions that frequently collect personal information or manage significant amounts of personal information or data.

6.12 Requests for Service, Enquiries and Correspondence

Council receives a significant number of requests for service, as well as general enquiries and correspondence, and a certain amount of personal information is required to be collected to allow Council to perform these functions.

These requests for service and enquiries are made:

- Over the phone (Council does not record telephone conversations; however, it does have a voicemail service);
- In writing (e-mail, letter, online or printed form); or
- In person (at Council's Customer Service Centre or other facilities).

Council determines the appropriate level of personal information to be collected for each type of service request and enquiry to allow sufficient information to be an accurate record of the issue and assistance given, but it will not collect unnecessary personal and/or health information.

If Council receives written correspondence, a full copy of whatever is sent is generally kept in Council's electronic document management system. The provision of any personal information is entirely voluntary, and in that respect personal information may be provided that is unsolicited.

Telephone conversations are not electronically recorded. If someone has an enquiry that cannot be answered straight away, the Council staff member will offer to take the person's name and telephone number or email address, so that another officer of Council can respond.

6.13 Complaints and Regulatory Functions

Council receives complaints from members of the public to investigate potential non- compliances with legislation, development consents, operating approvals etc. Most of these investigations are handled in accordance with the relevant legislation governing Council's activities in particular functions.

Council recognises that some people may wish to remain anonymous when making complaint, however, clear information regarding the consequences of remaining anonymous must be provided. For example, Council may not be able to properly investigate or consider a complaint or review a matter if sufficient information about the matter is not received. To appropriately investigate most matters, Council officers may be required to collect personal information from those parties involved, including names and addresses, but may also involve detailed correspondence or witness statements for complicated matters.

Council endeavours to maintain the confidentiality of complainants wherever possible, however, at times Council may be required to provide personal information of complainants to other parties due to legislative or court requirements.

6.14 Development Assessment and Land Use Planning

Anyone with an interest in a DA is welcome to make a submission or give feedback about a proposed development, but this must be done in writing. Any submissions made are public documents, and other people can view them on request.

6.15 Staff and Recruitment

Council collects personal and/or health information from staff members as part of its recruitment process. Council will never ask for more personal information than is required for that purpose.

Staff

During the recruitment process and throughout employment, information (including personal and/or health information) is collected from staff members for various reasons, such as leave management, workplace health and safety and to help Council to operate with transparency and integrity. Information collected by Council is retained, to the extent necessary and managed securely. In the exercise of its functions, Council collects and manages personal information about its staff including but not limited to:

- Medical conditions and illnesses;
- Next of kin contact details;
- Educational achievements;
- Performance and development information;
- Family and care arrangements;
- Secondary employment;
- Conflicts of interest and pecuniary interest disclosures;
- Banking details for payroll purposes;
- Employment history; and
- Details and copies of licences essential to the performance of an officer's role.

Recruitment

When someone applies for employment with Council, they send Council personal information, including their name, contact details and work history. Council provides this information to the interview panel for that position in electronic or hard copy files. The personal information is only used for the purposes of the recruitment process.

After recruitment is successful, applicants are required to fill out various forms to commence employment at Council. These forms require further personal and health information, such as the applicant's bank account details, tax file number, police clearance checks, emergency contacts and any disabilities that may impact their work. These forms are sent to the Human Resources unit to be used for employment purposes, such as payroll and setting up personnel files and the information is retained in secure storage systems.

6.16 Visitors and members of the public

When consultants, contractors and members of the public visit a Council facility they may be required to sign into the premises. The record of entry may be recorded in a physical sign-in register or via a digital QR Code check-in process.

During periods of health emergencies, Council may be required to provide check-in data for a facility to NSW Health, or any other relevant government agency. Council may be required to restrict entry or refuse provision of a service if the check-in process is not observed. Any check-in

data collected by Council will be held securely and destroyed on a regular basis in accordance with provisions under the *State Records Act 1998.* Check-in data collected by the Service NSW QR Code Check-In system will not be held by Council and will be held and stored by Service NSW.

6.17 Communications and stakeholder engagement

Subscriber, mailing and contact lists

Council offers residents and interested stakeholders the opportunity to stay up to date on the activities of Council via electing to subscribe to various e-newsletters produced by Council. These services are on an opt-in basis and personal contact information is supplied to Council voluntarily by subscribers. No personal information is collected without consent and those who provide their information are advised as to how Council will manage it. The information generally collected includes names and email addresses and in some cases areas of interest.

Community engagement and public consultation

Council regularly undertakes public consultation to help guide its decision-making and the provision of services. Council may collect information from you when you complete a survey or register for an event seeking public consultation.

6.18 Council Website and Service Providers

Council engages several service providers who provide software, website, internet services and computer systems through which Council may collect, store or process your personal information. On occasion our providers may have access to your personal information to facilitate services on behalf of Council. Council ensures that our providers adhere to the same legislative requirements in relation to Privacy as well as meet the requirements of this Plan.

Cookies

Council may use 'cookie' technology to collect additional website usage data and to improve its services. A cookie is a small piece of text sent to your browser by Council's website. This helps your website to remember your preferences and it makes your next visit easier and the site more useful to you. Council may use cookies for the following purposes:

- To better understand how you interact with Council services;
- To monitor aggregate usage by users and web traffic routing on Council services; and
- To improve Council services.

Most internet browsers automatically accept cookies. You can restrict that by editing your browser's options to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit.

6.19 Personal Contact Details

Council may engage service providers who assist Council in the distribution and communication of a variety of Council communication requirements. These may include printing and distribution of Council rate notices and Council newsletters etc. To facilitate this, Council service providers may be required to have access to personal information of residents and ratepayers to facilitate distribution of these materials on behalf of Council. Council ensures that its providers adhere to the same legislative requirements in relation to Privacy as well as meet the requirements of this Plan.

6.20 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.

Part 6 of the *PPIP Act* prevents Council employees from disclosing 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:

Register	**Primary Purpose of the register is to:**
Contracts Register	Identify all contracts over the value of $150,00 entered by Council
Graffiti Removal Register	Records the work carried out by Council under s 13 of the *Graffiti Control Act 2008*
Investments Register	Details of all investments currently held by Council
Land Register	Identify all land vested in Council, or under its control. The secondary purpose includes a consideration of public accountability as to the land held by Council.
Public Notification	Register of any notifications made under s 59N(2) *Register* of the *PPIP Act.* (To come into effect 28 November 2023).
Public Register	Identify all licences granted under s 308 the *of licenses Protection of the Environment Operations Act 1997*.
Record of building certificates	Identify all building certificates.
Records of approvals	Identify all approvals granted under the *LG Act. Record of impounding* Identify any impounding action by Council.
Register of disclosures	Identify applications for development consent and other *of* interest approvals, confirm determinations on appeal and identify applications for complying development certificates

Members of the public may enquire only in accordance with the primary purpose of any of these registers. Many of these registers are made available on Council's website, www.gisc.nsw.gov.au. If a register cannot be located on the website a request to see that register may be made to the Privacy Contact Officer via nambuccacouncil@nambucca.nsw.gov.au or in person at Council's Administration Centre, 44 Princess Street Macksville.

Secondary purpose of all public registers

Due to the general emphasis on local government processes and information being open and accountable, it is considered that a secondary purpose for which all public registers are held by Council includes the provision of access to members of the public. Therefore, disclosure of specific records from public registers would normally be allowable under s 57 of *PPIP Act*.

However, requests for access, copying, or the sale of the whole or a substantial part of a Public Register held by Council will not necessarily fit within this purpose. Council will make an assessment as to the minimum amount of personal information that is required to be disclosed

about any request and may seek a statutory declaration to satisfy itself as to the intended use of the information. Any request or application for government information will be assessed under the *Government Information (Public Access) Act 2009*.

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 Public Officer.

6.21 How to access and amend personal information

Council ensures that people can access information it holds about them. People have a right to amend their own personal or health information.

How do I access my own personal or health information?

Individuals wanting to access Council's records to confirm or amend their own personal or health information, such as updating contact details can do so by contacting Council either in person or in writing. Council will take steps to verify the identity of the person requesting access to information.

How do I amend my own personal or health information?

Individuals wanting to a amend their own personal or health information must put the request to Council in writing. This application must contain the following information:

- The full name, date of birth and contact details of the person making the request;
- State whether the application is under the *PPIP Act* or *HRIP Act;*
- Explain what personal or health information the person wants to amend; and
- Confirmation of the applicant's identity.

Accessing or amending other people's personal or health information

Council is restricted from giving individuals access to someone else's personal and health information unless that person provides Council with written consent. An "authorised" person must confirm their identification to act on behalf of someone else. There may be other reasons Council is authorised to disclose personal and 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.

6.22 Data Breaches

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 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.

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

6.23 How Council will manage a data breach

The Manager Information and Communication Technology will be promptly informed of any data breach and will assist in the assessment and management of the breach, including any reporting under NSW's voluntary data breach reporting scheme, in accordance with the IPC's Voluntary Data Breach Notification guidelines.

Mandatory Notification of Data Breach (MNDB) Scheme

Amendments to the *PPIP Act* will come into effect on 28 November 2023. The amendments impact the responsibilities of Council under the *PPIP Act* and require Council to provide notifications to affected individuals in the event of an eligible data breach of their personal or health information.

Under the MNDB Scheme Council will have an obligation to:

- Immediately make all reasonable efforts to contain a data breach;
- Undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach;
- During the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach;
- Decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach;
- Notify the Privacy Commissioner and affected individuals of the eligible data breach; and
- Comply with other data management requirements.

Prior to 28 November 2023, Council will adopt an updated Data Breach Policy and follow procedures under that Policy to ensure compliance with the obligations and responsibilities set out in Part 6A for the mandatory notification of data breach scheme.

The Policy will outline Council's overall strategy for managing data breaches from start to finish, and will enable Council to:

- Prepare for, evaluate, respond to and report on data breaches at the appropriate level and in a timely fashion;
- Mitigate potential harm to affected individuals and the Council; and
- Meet compliance obligations under the *PPIP Act*.

Council will include, at least the following in its DBP:

- How Council has prepared for a data breach.
- A clear description of what constitutes a breach.
- Strategy for containing, assessing, and managing eligible data breaches.
- Roles and responsibilities of staff members.
- Record keeping requirements.
- Post-breach review and evaluation.

6.24 Review rights and the complaint process

Council encourages individuals to try to resolve privacy issues informally before going through the formal review process to allow speedier resolution of concerns. Any person who may have a privacy concern can contact Council for advice or for referral to the Privacy Contact Officer.

6.25 Internal Review

Individuals have the right to seek an internal review under Part 5 of the *PPIP Act* if they believe 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 an authorised representative.

An application for internal review must be made to Council in writing within 6 months of when the affected person first became aware of the conduct or decision that is the subject of the application.

How does the process of Internal Review operate?

The Privacy Contact Officer or their delegate will conduct the internal review. If the internal review is about the conduct of the Privacy Contact Officer, the General Manager will appoint another person to conduct the internal review. The reviewing officer will refer to the Privacy Commissioner's guidance materials when carrying out an internal review.

Council will acknowledge receipt of an internal review within 5 working days and complete an internal review within 40 calendar days. Once the review is completed, Council may take no further action, or it may do one or more of the following:

- Make a formal apology;
- Take remedial action;
- Recommend alternative dispute resolution methods such as mediation or conciliation;
- Provide undertakings that the conduct will not occur again; and/or
- Implement administrative measures to reduce the likelihood of the conduct occurring again.

Within 10 working days of completing an internal review, Council will notify the applicant of the following:

- The findings of the review;
- The action proposed to be taken by Council and the reasons for taking that action (if any); and
- The right of the applicant to have those findings, and Council's proposed action, administratively reviewed by the NSW Civil and Administrative Tribunal.

6.26 The role of the Privacy Commissioner in the review process

The Privacy Commissioner has an oversight role in how privacy complaints are handled and is entitled to make submissions to Council regarding internal reviews. If Council receives an internal review application, it will:

- Notify the Privacy Commissioner of the application as soon as practicable;
- Keep the Privacy Commissioner informed of the progress of the internal review; and
- Inform the Privacy Commissioner of the findings of the review and the action proposed to be taken by Council in relation to the matter.

An individual can also make a complaint directly to the Privacy Commissioner about an alleged breach of their privacy.

6.27 External review by the NSW Civil and Administrative Tribunal (NCAT)

If the applicant disagrees with the outcome of an internal review or is not notified of an outcome within 40 calendar days (time allotted for a review) plus 10 working days (time allotted to notify the applicant of the review findings), they have the right to seek an external review and may make application to the NCAT for a review of Councils conduct. An application for external review can only be made after an internal review has been completed and must be made within 28 days from the date of the internal review decision.

6.28 Promoting Privacy

Compliance strategy

During induction, and on a regular basis, all employees will be made aware of this Plan and it will be made available on Council's Intranet and Council's website.

Council officials will be regularly acquainted with the general provisions of the *PPIP Act, HRIP Act*, this Plan, the IPPs, the Public Register provisions, the Privacy Code, and any other applicable Code of Practice.

Council utilises various collaborative tools for inductions, training and awareness programs such as virtual meetings and MS Teams Channels. The Privacy Contact Officer utilises these avenues, as well as face to face, to continually promote awareness and educate staff.

Council will utilise the Legislative Compliance Policy and the framework within to ensure compliance with the *PPIP Act* and *HRIP Act.*

Communication Strategy

Council will promote awareness of this plan and rights under *PPIP Act, HRIP Act* and this Plan to Council officials by:

- Providing an overview at inductions;
- Publishing the Plan on Council's internal and external websites;
- Offering training sessions as required;
- Providing specialised and on-the-job training to key groups; and
- Promoting the Plan regularly though newsletters, all staff emails, and initiatives such as Privacy Awareness Week.

Promoting the Plan to the Community

Council promotes public awareness of this Plan to the community by:

- Making it publicly available and publishing it on its website at www.gisc.nsw.gov.au;
- Writing the Plan in plain English;
- Telling people about the Plan when they enquire about personal and health information;
- Providing a link to the Information & Privacy Commission website [www.ipc.nsw.gov.au] and distributing copies of literature available on that site; and
- Including privacy statements on application forms and invitations for community engagement.

6.29 Privacy Impact Assessments

Council will endeavour to take a 'privacy by design' approach to ensure compliance with privacy

laws. Council will ensure that the privacy impacts of any new project or system development/implementation are thoroughly considered prior to implementation to allow issues of concern or risk to be addressed early in the process. Council will develop and implement an appropriate process for the assessment of privacy impacts of any new project or system development/implementation. The process will be guided by the NSW Privacy Commissioner's "Guide to Privacy Impact Assessments". A Privacy Impact Assessment shall be conducted whenever personal or health information will be collected, stored, used or disclosed in any project.

7.0 Legislation and Supporting Documents

Relevant Legislation, Regulations and Industry Standards include:

This Plan addresses the requirements of the *PPIP Act and* the *HRIP Act*. Please refer to "Appendix A" for more information about NSW's privacy laws, the IPPs and how these directly relate to the activities of Council.

7.1 External Contact Details

The Information and Privacy Commission NSW is the regulatory body overseeing the *GIPA Act*, the *PPIP Act* and the *HRIP Act*. Its website is located at www.ipc.nsw.gov.au and can be contacted for General enquires at:

Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 472 679
Address: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000
Postal: GPO Box 7011, Sydney NSW 2001

Disputes in relation to the *GIPA Act*, the *PPIP Act* and the *HRIP Act* are dealt with through the NSW Civil and Administrative Tribunal (NCAT). The NCAT website is located at www.ncat.nsw.gov.au. Contact details are provided on the website for the various registries.

The closest registry to Macksville is located at:

Newcastle Registry
Level 1, 175 Scott St, Newcastle NSW
Post: PO Box 792, Newcastle NSW 2300
Email: ccdnewcastle@ncat.nsw.gov.au- external site

To call the NCAT:
Telephone: 1300 006 228

8.0 Variation and Review

The Privacy Management Plan will be reviewed every three years, or earlier if deemed necessary, to ensure that it meets the requirements of legislation and the needs of Council. The term of the Plan does not expire on the review date, but will continue in force until superseded, rescinded or varied either by legislation or a new resolution of Council.

9.0 Reporting

Section 54 of the *PPIP Act* requires Council, as soon as practicable after receiving an application for an internal privacy review, to notify the NSW Privacy Commissioner of the application, keep the Commissioner informed of the progress of the internal review and inform the findings of the review and of the action proposed to be taken by the Council in relation to the matter.

The responsibility for providing such notifications to the NSW Privacy Commissioner lies with

Council's Privacy Contact Officer.

10.0 History

Department:	Corporate Services	**Last Reviewed**	**Resolution Number**
Policy Category	Council	24 April 2013	39/13 (CM10 8932/2013)
Endorsed By:	General Manager	11 January 2019	By AGMCS
Approval Authority	Council	11 October 2022	By AGMCS
Policy Owner	Director Corporate Services (DCS)	12 October 2023	
Contact Officer	Manager ICT		
Document No.	8961/2013		
First Adopted	1 November 2007		
Resolution No:	?		
Review Date:	October 2024		

Appendix A

ABOUT NSW'S PRIVACY LAWS

This section contains a general summary of how Council must manage personal and health information under the *PPIP Act*, the *HRIP Act* and other relevant laws. For more information, please refer directly to the relevant legislation or contact the Council.

The PPIP Act and personal information

The *PPIP Act* sets out how the Council must manage personal information.

About personal information

Personal information is defined in s 4 of the *PPIP Act* and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name and address, details about their family life, their sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, such as 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. Health information is generally excluded here as it is covered by the *HRIP Act*.

Information Protection and Health Privacy Principles

This section contains a general summary of how Council must manage personal and health information under the *PPIP Act* and *HRIP Act* and other relevant laws. *PPIP Act* provides for the protection of personal information by means of 12 IPPs and *HRIP Act* provides for the protection of health information by means of 15 Health Privacy Principles (HPPs).

Council complies with the IPPs prescribed under the *PPIP Act* and HPPs prescribed under *HRIP Act* as follows:

IPP 1 & HPP 1 Lawful Collection

Council will only collect personal and/or health information for a lawful purpose as part of its proper functions. Council will not collect any more information than is reasonably necessary to fulfil its proper functions. Such personal and health information may include names, residential address, phone numbers, email addresses, signatures, medical certificates, photographs and video footage (CCTV).

Anyone engaged by Council as a private contractor or consultant that involves the collection of personal and health information must agree to be bound not to collect personal information by any unlawful means. Any forms, notices or requests by which personal and health information is collected by Council will be referred to the Privacy Contact Officer prior to adoption or use.

IPP 2 & HPP 2 Direct Collection

Personal information will be collected directly from the individual unless that person consents otherwise. Parents or guardians may give consent for minors. Health information will be collected directly from the person concerned unless it is unreasonable or impracticable to do so. Collection may occur via phone, written correspondence to Council, email, facsimile, Council forms or in person. The Code makes provision for Council to depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.

Council may collect personal information from other public sector agencies in respect of specific statutory obligations where it is authorised by law to do so. The *PIPP Act* permits non-compliance with this principle if Council is exercising complaint handling, investigative functions or is authorised or required not to comply with the principle under any Act or law.

IPP 3 & HPP 3 Requirements when collecting

Council will inform individuals that their personal information is being collected, why it is being collected and who will be storing and using it. Council will also inform the person how they can view and correct their information.

A Privacy Statement is published on Council's website, intranet, included on forms where personal or health information is collected and available as a handout to the public.

Council will inform persons why health information is being collected about them, what will be done with it and who might see it. Council will also inform the person how they can view and correct their health information and any consequences if they do not provide their information. If health information is collected about a person from someone else, reasonable steps will be taken to ensure that the person has been notified as above.

IPP 4 & HPP 4 Relevance of collection

Council will seek to ensure that personal and health information collected is directly relevant to its functions, is accurate, and is up-to-date and complete. The collection will not be excessive or intrude into the personal affairs of individuals. Council will, under normal circumstances rely on the individual to supply accurate, complete information; although, in special circumstances some verification processes may be necessary.

IPP 5 & HPP 5 Secure storage

Council will store personal and health information securely, for no longer than as required by the General Retention and Disposal Authorities for Local Government Records issued by State Records Authority of NSW. It will then be disposed of appropriately. It will be protected from unauthorised access, use or disclosure by application of appropriate access levels to Council's electronic data management system and staff training.

If it is necessary for the information to be given to a person in connection with the provision of a service to the Council (e.g., consultants and contractors), everything reasonably within the power of the Council is done to prevent unauthorised use or disclosure of the information.

IPP 6 & HPP 6 Transparent access

Council will provide reasonable detail about what personal and/or health information is stored on an individual. Council stores information for the purpose of carrying out its services and functions and to comply with relevant record keeping legislation.

Individuals have a right to request access to their own information to determine what, if any information is stored, how long it will be stored for and how it is stored (e.g., electronically with open or restricted access to staff, in hard copy in a locked cabinet etc.).

Where Council receives an application or request by a person as to whether Council holds information about them, Council will undertake a search of its records to answer the enquiry. Council may ask the applicant to describe what dealings the applicant has had with Council to assist Council in conducting the search. Council will ordinarily provide a response to applications of this kind within 28 days of the application being made.

Council will issue a statement to be included on its website and in its Annual Report concerning the nature of personal information it regularly collects, the purpose for which the personal information is used and an individual's right to access their own personal information.

IPP 7 & HPP 7 Access to own information

Council will ensure individuals are allowed to access their own personal and health information without unreasonable delay or expense. Compliance with this principle does not allow disclosure of information about other people. If access to information that relates to someone else is sought, the application must be made under the *GIPA Act.*

Where a person makes an application for access under the *PPIP Act* and it is involved or complex, it may be referred, with the written consent of the applicant, as an application under the *GIPA Act*.

IPP 8 & HPP 8 Right to request to alter own information

Council will, at the request of a person, allow them to make appropriate amendments (i.e., corrections, deletions or additions) to their own personal and health information to ensure the information is accurate, relevant to the purpose for which it was collected, up to date and not misleading. Changes of name, address and other minor amendments require appropriate supporting documentation. Where substantive amendments are involved, an application form will be required, and appropriate evidence must be provided as to why the amendment is needed. If Council is unable to amend or delete the personal information a statement can be attached in such a manner as to be read with the information.

IPP 9 & HPP 9 Accurate use of information collected

Council will take all reasonable steps necessary to ensure personal and health information is accurate, relevant and up to date before using it. Council will consider the age of the information, its significance, the likelihood of change and the function for which the information was collected.

IPP 10 & HPP 10 Limits to use of information collected

Council will only use personal and health information for the purpose for which it was collected, for a directly related purpose or for a purpose for which a person has given consent. It may also be used without consent to deal with a serious and imminent threat to any person's life, health or safety, for the management of a health service, for training, research or to find a missing person.

Additionally, Council may use personal information to exercise complaint handling or investigative functions. The Code makes provision that Council may use personal information for a purpose other than the purpose for which it was created in the following circumstances:

- Where the use is in pursuance of Council's lawful and proper function/s and Council is satisfied that the personal information is reasonably necessary for the exercise of such function/s; and
- Where personal information is to be used for the purpose of conferring upon a person, an award, prize, benefit or similar form of personal recognition.

IPP 11 & HPP 11 Restricted and Limited disclosure of personal and health information

Council will only disclose personal and health information with the individual's consent or if the individual was told at the time of collection that it would do so. Council may also disclose information if it is for a related purpose and it considers that the individual would not object. Personal and health information may also be used without the individual's consent to deal with a serious and imminent threat to any person's life, health, safety, for the management of a health service, for training, research or to find a missing person.

The *PPIP Act* permits non-compliance of this principle if the disclosure is in relation to a complaint that is made to or referred from an investigative agency. The *PPIP Act* permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government (e.g., the Office of Local Government) if the disclosure is for the purposes of informing that Minister about any matter within that administration, or by a public sector agency under the administration of the Premier if the disclosure is for the purpose of informing the Premier about any matter.

Special limits on disclosure

Council will not disclose sensitive personal information without consent unless it is necessary to prevent a serious and imminent threat to the life or health of an individual, in relation to the following:

- Ethnic or racial origin;

- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership; and/or
- Health or sexual activities.

Council will not disclose this information to any person or body who is in a jurisdiction outside New South Wales unless:

- A relevant privacy law that applies to the personal information concerned is in force in that jurisdiction;
- The disclosure is permitted under a Privacy Code of Practice; and/or
- Council is requested by a potential employer outside NSW, it may verify that a current or former employee works or has worked for Council, the duration of that work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

Specific Health Information Privacy Principles

Health information includes information or an opinion about the physical or mental health or a disability of an individual and includes personal information about:

- A health service provided, or to be provided, to an individual;
- An individual's express wishes about the future provision of health services;
- Information collected in connection with the donation of human tissue; and/or
- Genetic information that is or could be predictive of the health of an individual or their relatives or descendants.

Health information is given a higher level of protection regarding use and disclosure than is other personal information. In addition to the principles, above, the following four additional principles apply specifically to health information:

HPP 12 Unique Identifiers

Council will only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the Council to carry out any of its functions efficiently.

HPP 13 Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering transactions with or receiving any health service(s) from Council.

HPP 14 Transborder data flow

Council will not transfer health information out of NSW without the individual's consent unless:

- Council is unable to obtain consent; it is of benefit to the individual and that they would likely give it;
- It is necessary for a contract with a third party;
- To help prevent a serious and imminent threat to life, health or safety of individuals;
- It is permitted by an Act or other law; or
- The recipient is subject to protection laws like the *HRIP Act*.

HPP 15 Cross-organisational linkages

Council does not participate in a system to link health records across more than one organisation currently. If Council decided to use a system like this in the future, Council would make sure that the individual to whom the health information relates expressly consents to the link.

How the Privacy Code of Practice for Local Government affects the Information Protection Principles

About IPPs 2, 3, 10 and 11, the Code makes provision for Council to depart from these principles where the collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.

About IPP 10, in addition to the above, the Code makes provision that Council may 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 function/s and Council is satisfied that the personal information is reasonably necessary for the exercise of such function/s.

About IPP 11, in addition to the above, the Code makes provision for Council to depart from this principle in the circumstances described below:

1. Council may disclose personal information to public sector agencies or public utilities on condition that:
   i) The agency has approached Council in writing;
   ii) Council is satisfied that the information is to be used by that agency for the proper and lawful function/s of that agency; and
   iii) Council is satisfied that the personal information is reasonably necessary for the exercise of that agency's function/s.
2. Where Council is requested by a potential employer, it may verify that a current or former employee works or has worked for Council, the duration of that work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

Offences

Offences can be found in Part 8 of the *HRIP Act*.

It is an offence for Council to:

- Intentionally disclose or use any health information about an individual to which the official has or had access to in the exercise of his or her official functions;
- Offer to supply health information that has been disclosed unlawfully;
- Attempt to persuade an individual to refrain from making or to withdraw an application pursuing a request for access to health information or a complaint to the Privacy Commissioner or Tribunal; or
- By threat, intimidation, or false representation require another person to give consent or to do, without consent, an act for which consent is required.

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

The *GIPA Act* provides a mechanism to access your personal information or other information. An application can be made to Council to access information that Council holds. Sometimes, this information may include personal and/or health information.

If a person has applied for access to someone else's information, Council will take steps to consult with people who might have concerns regarding disclosure of their personal information. Council will provide notice of the decision to ensure that people who might want to object to the release of information have time to apply for a review of the decision to release information.

State Records Act 1998 and State Records Regulation 2015

This law sets out when Council can destroy its records. It also authorises the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies, including Councils, manage their records appropriately.