

PRIVACY MANAGEMENT PLAN

Council policy - Version control information

Adopted by Council: 27 January 2021, Min No 10
Next review due: Nov 2025
Previous version(s): 23 April 2013, 23 June 2015
Policy register reference: 33
Responsible service: Governance and Civic Services

Contact position: Manager, Governance and Civic Services

Policy statement

Blue Mountains City Council (Council) will manage personal information in accordance with this Privacy Management Plan. This Plan relates to the collection, storage, access to, use and disclosure of personal information.

[Section 33](#) of the *Privacy and Personal Information Protection Act 1998* (NSW) ('PPIP Act') requires all councils to prepare a Privacy Management Plan outlining their policies and practices to ensure compliance with the requirements of that Act and the *Health Records and Information Privacy Act 2002* (NSW) ('HRIP Act'). This Plan has been prepared for the purpose of complying with section 33 of PPIP Act.

Scope

This policy explains how Council manages personal and health information. Personal and health information may relate to any person. This policy applies to all Council staff, Councillors, contractors and delegates in relation to the management of that information.

Roles and responsibilities

Position	Responsibility
Chief Executive Officer and executive	<ul style="list-style-type: none">To lead by example and demonstrate their active commitment to, and support for, the protection of privacy within and by Council.
Privacy Officers	<ul style="list-style-type: none">Oversight of privacy training with Council staff, Councillors and other Council officials as required;Review of relevant documents, application forms or other written requests by which personal or health information is collected by Council to ensure compliance with PPIP Act and HRIP Act (which may involve referral for legal advice or review);To oversee the implementation and management of the Privacy Statement and Privacy Management Plan;Conduct reviews and maintain compliance with the privacy complaint management processes and reporting to agencies;

	<p>and</p> <ul style="list-style-type: none"> To make recommendations on improvements, training or actions resulting from privacy complaints and/or reviews. The Privacy Officer may also provide opinions within Council on the application of the privacy principles. Any further concerns of a legal nature will be referred to Council's solicitor, and in the event of any residual doubts, the Privacy Officer will seek the opinion of the Information and Privacy Commission.
<p>All Council officials</p>	<p>This Plan applies in its entirety to Council officials, including Councillors and Council staff.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none"> Ensuring that all personal information is managed and secured in accordance with the privacy management plan and privacy principles; Undertaking appropriate privacy training on induction and at appropriate intervals based on role requirements, as recommended by the Privacy Officer; Seeking advice from the Privacy Officer, in particular at the project planning stage, regarding projects or forms that may involve the collection or disclosure of personal and/or health information; Immediately reporting any known or suspected breaches of any personal information to the Privacy Officer for assessment and advice on appropriate action; Ensuring all requests for a person's personal or health information are managed in line with approved processes or are referred to the Privacy Officer for assessment when required. <p>Council officials must act in manner that ensures compliance, this includes:</p> <ul style="list-style-type: none"> Ensuring information management is applied: Offences apply for the intentional unlawful disclosure or misuse of personal or health information, or an offer to unlawfully supply personal or health information under PPIP Act and HRIP Act, respectfully. Offences also apply under s664 of the Local Government Act. Reporting breaches: Any known or suspected breaches of this plan should be reported immediately to your supervisor or to Council's Privacy Officer. Maintaining confidentiality: The obligation of confidentiality is additional to and separate from that of privacy. An obligation of confidentiality exists for all staff whether express or implied as a matter of law.

Manager Business & Information Systems	<ul style="list-style-type: none"> To work with the Privacy Officer in relation to the assessment and resolution of data breaches.
--	---

Definitions

Term	Definition
Council	Blue Mountains City Council
Council official	Includes Councillors, members of staff of a Council, administrators, Council committee members, delegates of Council and advisors
Code of Conduct	The current <i>Code of Conduct</i> as adopted by Blue Mountains City Council.
collection (of personal information)	The way in which Council acquires personal or health information, which can include a written or online form, a verbal conversation, a voice recording, or a photograph.
disclosure (of personal information)	Occurs when Council makes known to an individual or entity personal or health information not previously known to them.
GIPA Act	<i>Government Information (Public Access) Act 2009</i> (NSW)
health information	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 the definition at S6 HRIP Act (see HRIP Act, s6 for the full definition).
HPE RM	Council's record management system.
HRIP Act	<i>Health Records and Information Privacy Act 2002</i> (NSW)
IPC	Information and Privacy Commission of NSW
personal information	<p>Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, including such things as an individual's fingerprints, retina prints, body samples, or genetic characteristics.</p> <p>Personal information is collected in various formats and may relate to any person, including but not limited to residents, customers, Council staff and Councillors.</p> <p>Exclusions to the definition of personal information are contained in s4(3) of the PPIP Act and includes health information. (see PIPP Act, s4 for the full definition).</p>
PIPP Act	<i>Privacy and Personal Information Protection Act 1998</i> (NSW)
Plan	This Privacy Management Plan
Privacy Code of Practice	Means the <i>Privacy Code of Practice for Local Government</i> made under Part 3 Division 1 of the PPIP Act.
Privacy Officer	Means Council's Manager Governance & Civic Services or as otherwise delegated by Council's Chief Executive Officer.

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. **HPERM: 20/116079**

privacy principles	The Information Protection Principles set out in Division 1 of Part 2 of the PIPP Act and Health Principles set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Within these principles lawful exemptions are provided. A summary is provided in Attachment 1 .
public register	A public register means a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee). Note: Public register exemptions are provided for in clause 7 of the Privacy and Personal Information Protection Regulation 2014.
staff	Paid employees of Council, volunteers, contractors and labour-hire staff.

Table of contents

1. Purpose.....	5
2. Implementation of this Plan	6
3. Council's responsibilities	6
4. About personal and health information	7
4.1 What is personal information.....	7
4.2 What is not personal information	7
4.3 Examples of personal information collected by Council.....	7
4.4 What is health information.....	7
4.5 Examples of health information collected by Council.....	8
5. How Council's actions relate to the Privacy Principles	8
5.1 Collection	8
5.2 Storage and disposal	10
5.3 Access and amendment.....	10
5.4 Use and accuracy of information	11
5.5 Disclosure of information.....	11
6. Privacy Protection Notice	12
7. Public registers.....	13
7.1 Public registers held by Council	13
7.2 Suppression of information.....	14
8. Privacy Breaches	14

8.1 Privacy and/or data breaches.....	14
8.2 How are data breaches of personal information managed?.....	15
9. Complaints and review rights.....	15
9.1 Privacy complaints	16
9.2 Internal review.....	16
9.3 External review by the NSW Civil and Administrative Tribunal (NCAT)	16
9.4 Complaints to the NSW Privacy Commissioner.....	17
10. Further information.....	17
Related documents	18
ATTACHMENT 1: PERSONAL AND HEALTH INFORMATION PROTECTION PRINCIPLES AND RELEVANT LEGISLATION	19
The Information Protection Principles	19
The Health Privacy Principles.....	21
Privacy codes of practice.....	23
Other relevant legislation.....	23

1. Purpose

Council collects, stores and uses a broad range of information. A significant part of that information is personal information. This Privacy Management Plan (this Plan) applies to that part of the Council’s information that is personal information.

The purpose of this Plan is to explain how Council manages personal and health information in accordance with NSW privacy laws, including the *Privacy and Personal Information Protection Act 1998* (PPIP Act); and *Health Records and Information Privacy Act 2002* (HRIP Act). This Plan is designed to inform:

- **The community** about how their personal information will be used, stored, amended and accessed after it is collected by the Council; and
- **Council officials** of their obligations in relation to handling personal information and when they can and cannot disclose, use or collect it.

This Plan also explains who you should contact with questions about the information collected and retained by Council, how to access and amend your stored information and how privacy complaints are handled, for example if Council may have breached the PPIP or HRIP Acts.

Additionally, this Plan is used to inform Council officials about how to deal with personal information. This helps to ensure that Council complies with the PPIP Act, the HRIP Act and the GIPA Act.

Section 33(2) of PPIP Act requires that this Plan must include:

The document on Council’s Records Management System is the controlled version. Please check that you have the current version before using a printed copy. **HPERM: 20/116079**

- Information about how Council develops policies and practices in line with the PIPP and HRIP Acts;
- 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 this Plan in relation to privacy and the personal and health information it holds.

Please refer to **Attachment 1** for more information about NSW's privacy laws and other relevant legislation.

2. Implementation of this Plan

This Plan will be made available on the Council's website and hardcopies will be kept at Council's offices for public reference as required. Council will inform people about this Plan when responding to enquiries about personal and health information.

All of the following persons will be made aware of this Plan and its availability, and provided a hardcopy by request:

- (a) all existing staff members;
- (b) all new staff members upon commencement of their positions at Council;
- (c) all Councillors;
- (d) all members of Council committees; and
- (e) any other relevant Council officials including administrators, delegates of Council and advisors.

This Plan will be used as a key resource in training Council officials on privacy matters.

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

- Endorsing this Plan at the elected Council level and making it publicly available;
- Offering training and advice to staff members as required;
- Providing a copy of this Plan to relevant oversight bodies such as the Audit and Risk Committee;
- Reporting on internal reviews to the Information and Privacy Commission; and
- Identifying privacy issues when implementing new systems, services and processes.

3. Council's responsibilities

The purpose of local government is to:

- Provide a representative, informed and responsible decision-making body;
- Develop the local community and its resources in a socially just and environmentally responsible way; and

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. HPERM: 20/116079

- Ensure that local public services and facilities respond effectively to community needs.

4. About personal and health information

4.1 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.

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

4.3 Examples of personal information collected by Council

Individuals may provide Council with personal information when they make enquiries and when Council delivers services to them. Examples of personal information may include:

- Names;
- Address and contact details, such as email and phone numbers;
- Signatures
- Date of birth and death
- Concession card details
- Opinions;
- Family relationship details;
- Housing, property or tenancy information;
- Health and fitness details; and
- Employment and education details.

Individuals also provide Council with personal information about other people in certain circumstances.

4.4 What is 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, results from drug and alcohol tests, and information about a person's medical appointments.

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. HPERM: 20/116079

See also the definitions of “personal information” and “health information” in the definitions table in this Plan.

4.5 Examples of health information collected by Council

The following is a list of examples of the types of health information and circumstances in which Council may collect health information:

- Seniors’ services where information may be collected on medical or support needs;
- Information on carers and families for the purposes of children’s services;
- Information on personal health and fitness for the purposes of gym membership;
- Volunteer programs where volunteers are asked to disclose health conditions which assist Council to provide support in the event of an incident or which may preclude them from some types of volunteer work;
- Information in relation to the need for assisted waste services;
- Information relating to staff health, for example medical certificates and workers’ compensation, fitness for duty assessments; and
- Medical certificates to the extent that they relate to public liability claims.

5. How Council’s actions relate to the Privacy Principles

Council will comply with the Information and Health Privacy Principles (**Attachment 1**). A brief summary of how this relates to our functions follows below. Further information is also provided on individual forms used for the collection of information.

The information practices relating to the collection, storage and use of personal or health information will be reviewed by the Council every four (4) years with the review of this Plan. Any new program initiatives will be incorporated into the review process with a view to ascertaining whether or not those programs comply with the PPIP Act.

5.1 Collection

Council collects and receives people’s personal and health information in a variety of ways, in order to perform services and functions.

Personal information may be collected electronically, in writing, over the telephone or in person. The collection of this information may be by:

- Application forms;
- Letters, email or fax;
- Online services such as Council’s website enquiry forms;
- Over the phone;
- In person including at Council’s office counters, or by Council officers visiting other sites, such as rangers and inspectors;
- Incident reports and medical assessment reports;

The document on Council’s Records Management System is the controlled version. Please check that you have the current version before using a printed copy. HPERM: 20/116079

- Submissions and other consultative mechanisms;
- CCTV or other audio or visual surveillance device footage and recordings;
- Financial transaction records; and
- Contracts.

Personal information may be collected from:

- Members of the public;
- NSW public sector agencies;
- Businesses;
- Non-government organisations;
- Staff and other Council officials; 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 responsibilities.

To this end, Council has a range of functions requiring or involving the collection of personal information, including:

- Levying and collecting rates;
- Providing services, for example, child care, libraries, waste collection, burial and cemetery services; and fitness and leisure services;
- Managing bookings for halls, sporting grounds and other Council facilities
- Consultation with the community, businesses and other stakeholders;
- Assessing development and 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 or grants;
- Employment; and
- Assessing fitness for work.

Council decides what level of personal or health information is appropriate to be collected for each enquiry on a case-by-case basis, with the understanding that the detail collected must contain enough information to be an accurate record of the issue and assistance given but should not contain unnecessary personal information.

Under section 10 of the PPIP Act, when Council collects personal information from an individual, it must make the individual aware of certain matters. This is done by way of a privacy protection notice. See **Part 6 of this Plan** for further information.

Treatment of unsolicited information

Where an individual, a group or committee, not established by Council, gives Council unsolicited personal or health information, then that information will still be treated in accordance with this Plan, the HRIP Act and the PPIP Act (for the purposes of IPPs 5 to 12 and HPPs 5 to 15) in relation to storage, access, use and disclosure of information.

Note that for the purposes of section 4(5) of the PPIP Act and section 10 of the HRIP Act personal or health information is not “collected” by Council if it is unsolicited.

5.2 Storage and disposal

Personal and health information is stored electronically and in physical files.

The following applies to information Council holds:

- Only Council staff, or delegated contractors such as auditors, can access personal information;
- Council officials will make reasonable efforts to ensure personal information is accurate before using it;
- Council officials will use personal information only for the purpose for which it was collected; and
- Council officials will not disclose personal information about a person to anyone without the consent of the person, or unless legally required or permitted to disclose information.

Electronic information is stored on secure information systems. Networks will be secure and require individual logins. New systems are assessed for compliance with the PPIP Act and HRIP Act. When not being used, hardcopy files and sensitive information are securely stored.

Information may be destroyed in accordance with the *State Records Act 1998* (NSW), Council’s *Records Management Policy* and the related document on *Normal Administrative Practice* for the management of records.

5.3 Access and amendment

The PPIP Act and the HRIP Act give people the right to confirm whether Council holds their own information and to access and amend that information.

Staff are only permitted to access personal or health information as it relates to the reasonable requirements of their role, and must appropriately manage conflicts at all time. Per Council’s *Workplace Surveillance Notification Policy*, audit trail information may be logged in relation to staff access to and amendment of data. Inappropriate access to or amendment of personal or health information will be treated as a conduct matter.

Members of the public wishing to access or amend personal and health information Council holds about them should contact Council using the contact information on the last page of

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

Limits on accessing or amending information

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

- a person can give Council consent to disclose their personal information to someone that would not normally have access to it ([PPIP Act, s26](#));
- an 'authorised person' can act on behalf of someone else ([HRIP Act, ss7 & 8](#)); and
- Council may be authorised to disclose 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.
- To 'amend' a record means that updated information may be saved to the relevant file as an updated record. Council may be unable to replace or destroy the previous record due to State Records Act requirements.

5.4 Use and accuracy of information

Staff use the personal and health information collected to:

- Deliver and continually improve services;
- Provide advice related to our services;
- Conduct research; and
- Assess infrastructure improvement priorities.

Staff and any other third party recipients of personal and health information held by Council are limited to using information only for the primary purpose(s) for which it was collected and as notified to the person supplying the personal information, or for such other use as permitted by legislation.

Council officials take reasonable steps to make sure that information is accurate before using it. Examples of how Council officials may do this include:

- Referring to primary sources before updating Council's Name and Address Register;
- Checking contact details directly with a person in the event of any doubts about accuracy, with file notes made of actions taken; and
- Checking the contents of letters prior to sealing them and checking attachments to emails.

5.5 Disclosure of information

Council does not disclose personal or health information it holds about staff or members of the public to external third parties without the individual's express consent unless it is legally authorised or required to do so. This includes authorisation to release information to other

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. HPERM: 20/116079

public sector agencies and utility providers in accordance with 4.12 of the *Privacy Code of Practice*.

Council also has discretion to, and can be required to, release personal information in relation to law enforcement, for example:

- In relation to proceedings for an offence including in response to a subpoena, search warrant or Order;
- To a law enforcement agency in relation to a person reported as missing
- If reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe that an offence has been committed;
- To assist another public sector agency that is an investigative agency in exercising its investigative functions.

Sensitive information

There are stricter obligations for the disclosure of personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health, and sexual activities. This information cannot be disclosed unless it is reasonably necessary for law enforcement purposes, or if the disclosure is necessary to prevent a serious or imminent threat to the life or health of a person.

6. Privacy Protection Notice

Under [section 10 of the PPIP Act](#), and [Schedule 1, 4\(1\) of the HRIP Act](#), when Council collects personal or health information from an individual, 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 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;
- Ways the individual can access and correct the information; and
- The name and address of the unit that is collecting the information and the unit that is to hold the information.

To ensure that Council complies with the PPIP Act, a *Privacy Protection Notice* will be included on all forms, letters and documents that are used to collect personal or health information from individuals.

The following is an example statement that will be used as a guide when developing new forms for use by Council that collect personal information. Forms should be signed and dated by the person to whom the information relates.

The personal information that Council is collecting from you is personal information for the purposes of the *Privacy and Personal Information Protection Act 1998* (PIIP Act).

Intended Recipients: The intended recipients of the personal information are: ***[[add or delete from examples list below as necessary]]***

- Officers within the Council;
- Other agent of the Council;
- Data service providers engaged by the Council from time to time; and
- *[[other entry as necessary]].*

Reason for collection: ***[[Complete as appropriate]]*** Council is collecting this personal information from you in order to *[[include explanation]].*

Supply: ***[[Complete as appropriate]]*** The supply of information by you is *[[voluntary]]* *[[mandatory]].* If you do not provide Council with this information, *[[include consequences of not including information, for example, that Council will be unable to provide certain services, or will/may not be able to process an application]].*

Access and Correction: You may make an application to access or amend information held by Council.

Storage: ***[[Select as appropriate]]*** *[[Council is the agency that holds and controls the information.]]* or *[[The agency which holds and controls the information is *[[insert]].*]]*

Enquiries: Contact *[[complete with name/position and contact details]].*

7. Public registers

Council is required by law to maintain a number of public registers and to make them available for public inspection. PIIP Act requires strict controls over the disclosure of information held in a public register.

7.1 Public registers held by Council

Examples of public registers which may contain personal or health information held by Council include, but are not limited to, the following:

- Public Land Register – *Local Government Act 1993*
- Contracts over \$150,000 awarded by Council – GIPA Act
- Register of Returns by Designated Persons – *Local Government Act 1993*
- Register of development consents and approvals – *Environmental Planning and Assessment Act 1979*
- Register of Planning Agreements - *Environmental Planning and Assessment Regulation 2000*
- Record of building certificates - *Environmental Planning and Assessment Act 1993*

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. **HPERM: 20/116079**

- Public record of licences held - *Protection of the Environment (Operations) Act 1997*
- Record of impounding – *Impounding Act 1993*

Enquiries about access to public registers can be made by contacting Council. Council staff members are prevented from giving access to information held on a public register if the purpose of the applicant seeking the information does not match the purpose for which the register is kept (Part 6 of the PPIP Act). Council may require a person seeking information on a public register to complete a statutory declaration stating the proposed use of that information ([s57\(2\) of the PPIP Act](#)), however this does not apply with respect to the inspection of the Register of Pecuniary Interest Returns ([Privacy Code of Practice](#) clause 5.2(1))

If the proposed use of the information is not related to the purpose of the register, access may be given at the discretion of Council but only in accordance with the *Privacy Code of Practice* concerning Public Registers.

7.2 Suppression of information

A person can apply to have information contained in material available for public inspection suppressed if the disclosure of that information would place the safety or well-being of a person at risk.

Applications for suppression of personal information should be made in writing to Council's Chief Executive Officer via Council's corporate contact details on the last page of this Plan. When in doubt, Council will err in favour of suppression.

8. Privacy Breaches

8.1 Privacy and/or 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 data. Examples include malware, hacking and data theft, accidental loss of a paper record, laptop, or USB stick, and emails sent to the wrong recipients if they contained classified material or personal information. All data breaches must be immediately reported to the Privacy Officer and Manager Business and Information Systems for analysis and appropriate action.

Data breaches may or may not also constitute a breach of privacy, depending on whether it involves personal information. A **privacy breach** may occur when personal information is disclosed or accessed in an unauthorised manner. Whether or not the breach of information is a privacy breach is for determination by the Privacy Officer and must be reported accordingly.

8.2 How are data breaches of personal information managed?

Council will determine whether personal information has been accessed to determine what response should be taken. The Privacy Officer will determine the seriousness of a breach by:

- Considering the type of data held;
- Whether personal or health information was disclosed;
- The number of individuals affected; and
- The risk of harm that could be caused to both individuals and Council by the breach.

After the seriousness of a breach has been determined, Council will take the following steps to manage a data breach of personal information:

1. **Contain:** Steps will be taken to contain the breach and minimise any resulting damage.
2. **Evaluate:** The type of data involved in the breach will be assessed, and the risks associated with the breach, to determine next steps. This will include an assessment of who is affected by the breach, what was the cause of the breach, and any foreseeable harm to the affected individuals/organisations.
3. **Notify:** Individuals/organisations affected by the breach will be notified as soon as possible to enable them to take any steps required to protect themselves, and to advise them of their rights to lodge a complaint with the Privacy Commissioner. Council's default position is to voluntarily report data breaches to the Privacy Commissioner. If there are good reasons not to do so these will be recorded in Council's internal report of the breach. Note that some mandatory or voluntary reporting of privacy breaches may apply. For example, Council may have notification obligations under the Notifiable Data Breaches (NDB) scheme, in the federal *Privacy Act 1988* (Privacy Act). Council will follow legislative requirements in relation to the voluntary or mandatory reporting of data breaches. Further information is available on the [IPC's website](#).
4. **Act:** Any additional action identified to mitigate risks will be implemented.
5. **Prevent:** Preventive efforts will be put into action based on the type and seriousness of the breach.

9. Complaints and review rights

Council encourages the informal resolution of privacy issues before going through the formal internal review process. A person can contact Council by phone and speak with the Privacy Officer. A person can also write a letter to or email Council with their concerns and Council will respond providing advice on the best course of action. Please refer to the contact details for Council at the end of this Plan.

9.1 Privacy complaints

Privacy complaints which do not request internal review will be managed in accordance with Council's customer service standards and *Complaints Handling Policy*. Internal reviews are not automatic, but are triggered by a specific request made by an individual as outlined below.

9.2 Internal review

Individuals have the right to seek an internal review under Part 5 of the PIPP Act if they believe that Council has breached the PPIP Act or the HRIP Act with respect to their own personal or health information. Individuals cannot seek an internal review for a breach of someone else's privacy, unless they are an authorised representative of the other person.

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 Privacy Officer. The [Privacy Internal Review Form](#) prepared by the Information and Privacy Commission may be used.

The Privacy Officer will usually conduct the internal review unless the internal review is about the conduct of the Privacy Officer. In this case Council will appoint another suitable person to conduct the internal review.

An internal review checklist has been prepared by the Information Privacy Commission and can be accessed from its website www.ipc.nsw.gov.au/. The reviewing officer will refer to the Information and Privacy Commissioner's guidance materials when carrying out an internal review.

Council will:

- Acknowledge receipt of an internal review within **5 working days**;
- As soon practicable after receiving the application notify the Privacy Commissioner of the application;
- Complete an internal review within **60 calendar days**.

The Privacy Commissioner is entitled to make submissions to Council regarding internal reviews. The Council officer conducting the internal review must consider any relevant material submitted by the applicant or the NSW Privacy Commissioner in reviewing the subject of the application.

The applicant will be notified of the outcome of the internal review within 14 days of its determination.

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

If an applicant is unsatisfied with the findings of the internal review or is not notified of the outcome of an internal review within 60 days, they have 28 days (see [Rule 24 of the Civil](#)

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. HPERM: 20/116079

[and Administrative Tribunal Rules 2014 \(Amendment No 2\)](#)) to ask the NSW Civil and Administrative Tribunal (NCAT) to review the conduct or decision complained about.

9.4 Complaints to the NSW Privacy Commissioner

Privacy complaints of a general nature may also be made to the NSW Privacy Commissioner. See www.ipc.nsw.gov.au for further information or refer to the IPC contact details at this end of this Plan.

10. Further information

For assistance in understanding the processes under the PPIP Act and the HRIP Act, please contact Blue Mountains City Council or the Information and Privacy Commission NSW.

Blue Mountains City Council
Attention: Privacy Officer
Blue Mountains City Council
Locked Bag 1005
Katoomba NSW 2780

Email: council@bmcc.nsw.gov.au
Phone: 02 4780 5000

Information and Privacy Commission NSW
Privacy Commissioner
GPO Box 7011
Sydney NSW 2001

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

NSW Civil and Administrative Tribunal (NCAT)
Principal Registry
Level 9, John Maddison Tower
86-90 Goulburn Street, Sydney NSW 2000

Email: ncathelpdesk@ncat.nsw.gov.au
Phone: 1300 006 228

Related documents

This document should be read in conjunction with:

Legislation

- [Privacy and Personal Information Protection Act 1998 \(NSW\)](#)
- [Health Records and Information Privacy Act 2002 \(NSW\)](#)
- [Local Government Act 1993 \(NSW\)](#)

Other documentation

- Blue Mountains City Council, *Code of Conduct*
- Blue Mountains City Council, *Records Management Policy*
- Blue Mountains City Council, *Complaints Handling Policy*
- Information and Privacy Commission, *Privacy Code of Practice for Local Government (December 2019)*

ATTACHMENT 1: PERSONAL AND HEALTH INFORMATION PROTECTION PRINCIPLES AND RELEVANT 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* (PIPP Act), the *Health Records and Information Privacy Act 2002* (HRIP Act) and other relevant legislation.

The Information Protection Principles

The PPIP Act provides for the protection of personal information by means of 12 Information Protection Principles ('IPPs'). These principles are as follows. Please note that certain statutory exemptions to these principles may apply.

Collection

1. Council will only collect personal information for a lawful purpose, and which directly relates to its functions. Council will collect only as much information as is reasonably necessary for that purpose.
2. Council will only collect personal information directly from a person. Exceptions to this include: (a) where an individual has authorised collection from someone else; (b) where the person is under 16 years of age and information has been collected by a parent or guardian or the person; or (c) where indirect collection is necessary when an award, prize or benefit is intended to be given to the person.
3. Council will give certain information to people from whom they collect personal information. Namely: (a) that information is being collected; (b) why it is being collected; (c) to whom the information will be disclosed; (d) whether the collection of the information is voluntary or required by law and whether there are any consequences for not providing the information; (e) regarding rights to access or amend the information. Council may depart from this principle if the information is being collected for an award, prize or benefit to be given to a person.
4. Council will ensure that personal information collected is relevant, accurate, complete and not excessive. Council will ensure that collection of information does not unreasonably intrude into a person's affairs.

Storage

5. Council will keep personal information secure, protect it against loss, unauthorised use or disclosure, and dispose of it securely and in accordance with any requirements for the retention and disposal of [personal information](#) when it is no longer necessary.

Access and accuracy

6. Council will take reasonable steps to enable a person to find out about the personal information it holds, the purposes for which the information is used, and how a person may gain access to their information held by Council, in accordance with Council's Code of Conduct, approved policies and recorded procedures. Council will maintain a statement on its website about the information it holds, and include a statement in its

annual report.

7. Council will allow people to access their own personal information held by Council without excess delay or expense. A person has the right to insist that their application for their own personal information is made under the PPIP Act. An application under the Government Information (Public Access) Act 2009 (NSW) ('GIPA Act') may be made as a last resort. Please use the [Application to Access Information form](#) on Council's website or contact Council for further information.
8. Council will allow people to update, amend or correct their personal information as necessary. Council will not charge a person to amend a record.
9. Council will take reasonable steps to ensure that personal information is relevant, accurate, up-to-date and not misleading before using that information.

Use

10. Council will only use personal information for the purpose for which it was collected unless it has consent to use it for another purpose. Council may use information other than for the original purpose, so long as it is consistent with Council's lawful and proper functions and is reasonably necessary for such functions, or when an award, prize or benefit is intended to be given to the person.

Disclosure

11. Council will not disclose a person's personal information without consent, unless otherwise permitted under the PPIP Act or other legislation. Council may disclose information to a public sector agency or public utility if that agency has approached Council in writing and Council is satisfied that the disclosure of the information is reasonably necessary and for the proper or lawful functions of that agency. A further exception applies where the information has been collected with the intention of giving an award, prize or benefit to the person.
12. Council will not disclose sensitive personal information. This includes personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

Offences

Offences can be found in [s62-68 of the PPIP Act](#).

It is an offence to:

- intentionally disclose or use personal information for an unauthorised purpose;
- offer to supply personal information that has been disclosed unlawfully; or
- hinder the NSW Privacy Commissioner or their staff from doing their job.

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. **HPERM: 20/116079**

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; and
- Council is not required to comply with IPP 2 if the information concerned is collected in relation to court or tribunal proceedings.

The Health Privacy Principles

The HRIP Act provides for the protection of health information by means of 15 Health Privacy Principles (HPPs). Those principles are as follows. Please note that certain statutory exemptions to these principles may apply.

Collection

1. Council will only collect information for a lawful purpose, and which directly relates to its functions. Council will collect only as much information as is reasonably necessary for that purpose.
2. Council will ensure that health information is relevant, accurate, is not excessive and does not unreasonably intrude into people's personal affairs.
3. Council will only collect health information directly from the person concerned, unless it is unreasonable or impractical to do so.
4. Council will give certain information to people from whom they collect health information. Namely: (a) the identity of Council and how to contact Council; (b) the reason why health information is being collected and who that information will be disclosed to; (c) information regarding rights to access the information; and (d) whether the collection of the information is voluntary or required by law and whether there are any consequences for not providing the information.

Storage

5. Council will keep health information secure, protect it against loss, unauthorised use or disclosure, and dispose of it securely and in accordance with any requirements for the retention and disposal of [health information](#) when it is no longer necessary.

Access and accuracy

6. Council will take reasonable steps to enable a person to find out about the health information it holds, the purposes for which the information is used, and how a person may access it.
7. Council will allow people to access their own health information held by Council without excess delay or expense. Please contact Council for further information.

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. HPERM: 20/116079

8. Council will allow people to update, amend or correct their health information as necessary.
9. Council will take reasonable steps to ensure that health information is relevant, accurate, up-to-date and not misleading before using that information.

Use

10. Council will only use health information for the purpose for which it was collected unless it has consent to use it for another purpose.

Disclosure

11. Council will not disclose a person's health information without consent, unless otherwise permitted under the HRIP Act or other legislation

Identifiers and anonymity

12. Council may use unique identifiers for individuals if reasonably necessary to carry out its functions efficiently.
13. Council will allow people to remain anonymous where it is lawful and practicable.

Information transfers and linkage

14. Council will not transfer health information outside NSW except as permitted under HRIP Act. Council does not usually transfer health information outside of NSW.
15. Council will not include health information of an individual in a health linkage system unless the person has given their express consent to that link. Council does not currently use a health information linkages system.

Offences

Offences can be found in [s68-70 of the HRIP Act](#).

It is an offence to:

- intentionally disclose or use health information for an unauthorised purpose;
- offer to supply health information that has been disclosed unlawfully.

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.

Privacy codes of practice

Council is subject to the *Privacy Code of Practice* as prepared by the Office of the Privacy Commissioner.

Under the *Privacy Code of Practice*, and 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. This Code 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.

Other relevant legislation

This section contains information about other relevant legislation.

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.

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.

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.

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.

Referrals to external agencies under other relevant legislation

Under the *Ombudsman Act 1974*, the *Independent Commission Against Corruption Act 1998*, and the *Crimes Act 1900* Council can provide information to the:

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

The document on Council's Records Management System is the controlled version. Please check that you have the current version before using a printed copy. HPERM: 20/116079