

Privacy Management Plan

Practices and procedures
governing the handling of
personal information and
privacy complaints
management



ROUS
COUNTY COUNCIL

Contact details for further information

Rous County Council's Privacy Contact Officer

(02) 6623 3800

council@rous.nsw.gov.au

www.rous.nsw.gov.au

PO Box 230, Lismore NSW 2480

Information and Privacy Commission

1800 472 679

ipcinfo@ipc.nsw.gov.au

www.ipc.nsw.gov.au

GPO Box 7011, Sydney NSW 2001

New South Wales Civil and Administrative Tribunal

1300 006 228 Select option 3 for Administrative and Equal
Opportunity Division enquiries

13 14 50 Interpreter Service (TIS)

1300 555 727 National Relay Service

NSW Civil and Administrative Tribunal Administrative and
Equal Opportunity divisions

PO Box K1026, Haymarket NSW 1240

DX 11539 Sydney Downtown

CM: [D22/21198 - Revised Privacy Management plan](#)

Review frequency: 4 years

Version	Purpose and description	Date approved by GM
1.0	Review of the Privacy Management policy (2015: for the three counties) resulted in the creation of a Privacy policy and separate Privacy Management Plan.	27-09-2022 by email (refer to note in CM D22/21198 - Revised Privacy Management plan).
2.0	The introduction of the Mandatory Notification of Data Breach Scheme led to the review and update of this Privacy Management Plan	21-11-2023 by email

Definitions

GIPA Act	means the <i>Government Information (Public Access) Act 2009</i> (NSW)
HPP	means 'Health Privacy Principle'
HRIP Act	means the <i>Health Records and Information Privacy Act 2002</i> (NSW)
IPP	means 'Information Protection Principle'
LG Act	means <i>Local Government Act 1993</i> (NSW)
PPIP Act	means <i>Privacy and Personal Information Protection Act 1998</i> (NSW)
Privacy Code	means <i>Privacy Code of Practice for Local Government</i>

Related documents

[Data Breach Plan](#)

[Privacy Complaint: Internal Review Application Form](#)

[GIPA application form](#)

[Privacy Management policy](#)

Contents

Part 1: Introduction	6
Part 2: What is personal and health information?	6
2.1 What is 'personal information'?	6
2.2. What is not 'personal information'?	6
2.3. What is 'health information'?	7
2.4. What is not 'health information'?	7
2.5. Personal and health information held.....	7
2.6 Information held when exercising functions on behalf of third parties	8
Part 3: What responsibilities do people have?	8
3.1. General Manager and Leadership Team.....	8
3.2. Employees, contractors and service providers	8
3.3. Managers and supervisors	9
3.4. Privacy Contact Officer.....	9
3.5. Governance and Risk.....	9
3.6 IT Team	9
Misuse of information	9
Part 4: How do the privacy principles apply?	10
4.1. Exemptions.....	10
4.2. IPP 1 and HPP 1: Collection of personal and health information for lawful purposes	11
4.3. IPP 2 and HPP 3: Collection of personal and health information from the individual to whom the information relates.....	11
4.4. IPP 3 and HPP 4: Requirements when collecting personal and health information	12
4.5. IPP 4 and HPP 2: Other requirements relating to the collection of personal and health information.....	12
4.6. IPP 5 and HPP 5: Retention and security of personal and health information	12
4.7. IPP 6 and HPP 6: Information about personal and health information held	13
4.8. IPP 7 and HPP 7: Access to own information.....	13
4.9. IPP 8 and HPP 8: Correction or alteration of own personal and health information.....	13
4.10. IPP 9 and HPP 9: Accuracy of personal and health information before use of information .	14
4.11. IPP 10 and HPP 10: Limits on use of personal and health information	14
4.12. IPP 11 and HPP 11: Limits on disclosure of personal and health information	14
4.13. IPP 12: Special limits on disclosure of personal information	15
4.14. HPP 12: Unique identifiers	15
4.15. HPP 13: Anonymity.....	15
4.16. HPP 14: Transfer of data flow.....	15
4.17. HPP 15: Cross-organisational linkages.....	16
Part 5: Registers	16
5.1. Definition	16
5.2. Disclosure of personal information contained in registers	16
5.3 Application to suppress information (not public registers)	16

5.4	Application to suppress information (public registers).....	17
Part 6: Privacy complaints and review options		17
6.1.	Internal review process	17
6.2.	External review process	18
6.3.	Other options	18
Part 7: Other information		19
7.1	Training	19
7.2	Unsolicited information	19
7.3.	Public consultation processes	19

Part 1: Introduction

Rous County Council is a 'public sector agency' as defined in the PPIP Act. This means we are required to have a Privacy Management Plan (PMP) setting our commitment to respecting the privacy rights of various individuals. This PMP is made pursuant to section 33 of the PIPP Act and should be read in conjunction with the Privacy policy and the Data Breach Plan. The preparation of the PMP has been informed by and based on the Model Privacy Management Plan for Local Government prepared by the NSW State Government. The objectives of the PMP are to:

- Establish governance arrangements that aim to protect an individual's personal and health information, and
- Inform the community about how their personal and health information will be used, stored and disclosed in the course of our operations.

The PMP applies to:

- Councillors
- Council employees
- Consultants and contractors of Council
- Council owned businesses, and
- Council Committees, including those established under the LG Act and extends to community members of such committees.

We consider the requirements of the PPIP Act and HRIP Act during the review and preparation of all policy, procedure and forms to ensure that we are satisfying our privacy obligations.

NOTIFICATION OF DATA BREACHES –

Council's plan for responding to and notifying affected individuals/organisations of data breaches relating to their personal information is contained in the Data Breach Plan (DBP). Council is required to have a DBP in accordance with the requirements of the Mandatory Notification of Data Breach (MNDB) scheme under Part 6A of the PPIP Act.

Part 2: What is personal and health information?

2.1 What is 'personal information'?

See section 4 of the [PPIP Act](#).

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. It includes things like an individual's fingerprints, retina prints, body samples or genetic characteristics.

2.2. What is not 'personal information'?

See section 4 of the [PPIP Act](#).

The PPIP Act outlines many examples of what is not personal information. One example is information about an individual that is contained in a publicly available publication. Once personal information is contained in a publicly available publication, it ceases to be covered by the PPIP Act.

Examples of publicly available publications:

- An advertisement containing personal information in a local, city or national newspaper
- Personal information on the internet including a website and social media platforms
- Books or magazines that are printed and distributed broadly to the general public

- Council Business Papers or that part that is available to the public, and
- Personal information that may be part of a public display on view to the general public.

Where an individual requests access to information that has already been published, we will rely on the provisions of the relevant Act that authorises Council to hold that information and not the PPIP Act (for example, an informal request under the GIPA Act).

2.3. What is ‘health information’?

See section 6 of the [HRIP Act](#).

- (a) Information or an opinion about:
 - (i) The physical or mental health or a disability (at any time) of an individual, or
 - (ii) The individual’s express wishes about the future provision of health services to him or her, or
 - (iii) A health service provided, or to be provided, to an individual, or
- (b) Other personal information collected to provide, or in providing, a health service, or
- (c) Other personal information about an individual collected in connection with the donation, or intended donation, of an individual’s body parts, organs or body substances, or
- (d) Other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or
- (e) Healthcare identifiers.

2.4. What is not ‘health information’?

See section 6 of the [HRIP Act](#).

Health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIP Act generally or for the purposes of specified provisions of the HRIP Act.

2.5. Personal and health information held

We perform various functions associated with bulk water supply, weed biosecurity and flood mitigation including water testing. This means we collect a range of personal and health information directly related and incidental to the performance of day-to-day activities. For example, handling enquiries and complaints, managing and supporting our workforce including recruitment, performing various financial administrative functions associated with the engagement, management and payment of third parties.

For employees, it includes:

- Recruitment material
- Leave and payroll data
- Personal contact information
- Performance management plans and disciplinary information
- Returns of interests (designated persons)
- Wage and salary entitlements
- Information collected in accordance with Council’s Workplace Surveillance policy
- Drug and alcohol testing information
- Health monitoring information
- Injury management and return to work plans
- Union membership
- Site attendance or check-in information (e.g., COVID Safe Check-in or similar)

- Health information (i.e., pre-employment medical information, health monitoring information, medical certificates and workers' compensation claims).

For councillors, it includes:

- Personal contact information
- Complaints and disciplinary matters
- Returns of interests
- Site attendance or check-in information (e.g., COVIDSafe Check-in or similar).

For other people, includes:

- Site attendance or check-in information (e.g., COVIDSafe Check-in or similar)
- Rates records
- Bank details
- Personal contact information
- Concession information
- Various types of health information incl. information voluntarily disclosed through public consultation processes.

2.6 Information held when exercising functions on behalf of third parties

We may, from time to time, exercise functions under delegation or by agreement for other organisations including local councils, NSW government agencies and non-government entities. This may involve the collection and storage of personal and/or health information. When exercising such functions we are responsible for complying with privacy obligations in terms of the personal information that is collected, stored and processed on behalf of that third party, including ensuring data security and data quality. We can share information we obtain with the third party, without separately requesting consent from the owner of the information.

When exercising functions for a third party we will only handle personal and health information in accordance with any relevant instrument of delegation or agreement. Third parties for whom we are exercising functions may specify matters such as the applicable retention periods, security requirements and contents of privacy collection notices.

Part 3: What responsibilities do people have?

3.1. General Manager and Leadership Team

- Ensure the effective implementation of the Privacy policy and PMP within areas of responsibility.
- Ensure adequate controls are implemented and maintained to safeguard information.
- Ensure that there are adequate resources for training of Privacy Contact Officers and staff.

3.2. Employees, contractors and service providers

- Ensure own compliance with information handling and management requirements, including preventing the unauthorised disclosure of personal or health information to whom the policy applies.
- Report any instances of known or suspected unauthorised disclosure.
- Ensure appropriate security and access controls are in place to ensure confidentiality of information.

3.3. Managers and supervisors

- In addition to their responsibilities as employees, managers and supervisors are responsible for ensuring awareness of, and compliance with, the Privacy policy and PMP.

3.4. Privacy Contact Officer

- Ensuring the PMP is up to date.
- Socialising the PMP.
- Communicating changes to the PMP.
- Primary contact for members of the public and the Information and Privacy Commission with respect to privacy and personal information related matters.
- Primary contact within and internal advisor on all matters related to privacy and personal information.
- Handle and respond to privacy complaints, and
- Perform compliance assurance checks and report results on privacy incidents, complaints and other relevant metrics.

3.5. Governance and Risk

- The Governance Risk team is responsible for managing our privacy management functions, including internal privacy reviews.

3.6 IT Team

- In addition to their responsibilities as employees, the IT team are responsible for the maintenance and security of our IT systems, including ensuring that the security and access controls are appropriate and effective.

Misuse of information

A public official who intentionally discloses personal or health information to which the official has or had access to in the exercise of their functions is guilty of an offence (see PPIP Act and HRIP Act). Additionally, any person attempting to induce a public sector official to disclose personal or health information is also guilty of an offence.

The PPIP Act and HRIP Act also make it an offence to offer to supply personal or health information that the person knows, or reasonably ought to have known has been disclosed in contravention of PPIP Act or HRIP Act.

Penalties include fines and imprisonment.

Part 4: How do the privacy principles apply?

4.1. Exemptions

We will comply with the IPPs and HPPs, unless an exemption applies. It is important to note that the PMP does not cover all exemptions or situations and should be used as a guide only.

Ref	IPP Exemptions	Notes
A	Relating to law enforcement and related matters.	Section 23 of the PIPP Act
AA	Relating to ASIO.	Section 23A of the PIPP Act
B	The information is reasonably necessary in order to enable Council to exercise its complaint handling functions or any of its investigative functions.	Section 24 of the PPIP Act
C	Where non-compliance is lawfully authorised or required.	Section 25 of the PPIP Act.
D	Where non-compliance would benefit the individual concerned.	Section 26 of the PPIP Act.
E	Relating to information exchanges between public sector agencies.	Section 27A of the PPIP Act.
F	Relating to research.	Section 27B of the PPIP Act.
G	Relating to emergency situations.	Section 27D of the PPIP Act.
H	The disclosure is made to a public sector agency under the administration of the Minister for Local Government or a public sector agency under the administration of the Premier for the purpose of informing the Minister or Premier about any matter within their respective jurisdictions.	Section 28 of the PPIP Act.
I	The disclosure of personal information for research purposes is in accordance with any applicable direction made by the Privacy Commissioner or any Research Code of Practice made by the Attorney General.	Section 41 of the PPIP Act.
J	Relating to the disclosure of personal information for Council's lawful and proper function/s.	Section 8 of the PPIP Act.
K	If collection 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.	IPP2, IPP3 in Privacy Code.
L	Relating to the disclosure of personal information to other public sector agencies or public utilities	IPP11 in Privacy Code.
M	Relating to the disclosure of personal information to potential employers.	IPP11, IPP12 in Privacy Code.

Ref	HPP Exemptions	Notes
1	Relating to the management of health services.	Schedule 1 of the HRIP Act and the Statutory Guidelines on the Use or Disclosure of Health Information for the Management of Health Services.
2	For training purposes.	Schedule 1 of the HRIP Act and the Statutory Guidelines on the Use or Disclosure of Health Information for Training Purposes.
3	For research purposes.	Schedule 1 of the HRIP Act and the Statutory Guidelines on the Disclosure of Health Information for Research Purposes.
4	Relating to the collection of health information from a third party.	Schedule 1 of the HRIP Act and the Statutory Guidelines on the Use or Disclosure of Information from a Third Party.

Relevant legislation permitting non-compliance with IPPs or HPPs

- *Crimes Act 1900*
- *Data Sharing (Government Sector) Act 2015*
- *General Data Protection Regulation*
- *GIPA Act*
- *Government Information (Information Commissioner) Act 2009*
- *Independent Commission Against Corruption Act 1988*
- *Local Government Act 1993*
- *Public Interest Disclosures Act 1994*
- *State Records Act 1998.*

Relevant Codes of Practice or public interest directions

- Privacy Code of Practice for Local Government
- Statutory Guidelines on the Use or Disclosure of Health Information for the Management of Health Services (HRIP Act)
- Statutory Guidelines on the Use or Disclosure of Health Information for Training Purposes (HRIP Act)
- Statutory Guidelines on the Disclosure of Health Information for Research Purposes (HRIP Act)
- Statutory Guidelines on the Use or Disclosure of Information from a Third Party (HRIP Act).

4.2. IPP 1 and HPP 1: Collection of personal and health information for lawful purposes

We will:

- only collect personal and health information for a lawful purpose that directly relates to our functions
- use a variety of methods to notify individuals that their information is being collected including:
 - o verbally
 - o via forms completed by individuals
 - o by correspondence (both electronically and in physical form).

We will not:

- collect personal or health information by any unlawful means
- collect any more personal or health information than is reasonably necessary to fulfil our proper functions.

Exemptions

Nil.

4.3. IPP 2 and HPP 3: Collection of personal and health information from the individual to whom the information relates

We will:

- collect information only from the individual to whom the information relates unless the individual has authorised collection from someone else or the information has been provided by a parent or guardian of a person under the age of 16 years
- only collect health information directly from the individual that the information concerns unless it is unreasonable or impractical for us to do so
- collect this information:
 - o verbally
 - o via forms completed by individuals

- o by correspondence (both electronically and in physical form).

Exemptions

A, B, C, D, E, G, K.

4.4. IPP 3 and HPP 4: Requirements when collecting personal and health information

We will:

- inform individuals that their personal and health information is being collected, why it is being collected, who will be storing and using the information, the name and address of the agency that has collected the information, and the agency that is to hold the information
- inform individuals of how they can view and correct their information, if the information is to be provided on a voluntary or mandatory basis and any consequences the individual may face if they do not provide the information
- where we collect personal and health information indirectly from someone else in respect of any one of our statutory functions, advise those individuals that we have collected their personal information (e.g., information collected from Land and Property Information about ownership details when a land is transferred from one owner to the next).

Exemptions

A, B, C, D, E, F, G, I, K.

4.5. IPP 4 and HPP 2: Other requirements relating to the collection of personal and health information

We will:

- take reasonable steps to ensure that personal and health information collected:
 - o is relevant to our functions, is not excessive, and is accurate, up to date and complete, and
 - o does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates by ensuring that it is only collected directly from the individual concerned
- ensure that all forms used by us comply with IPP 4 and HPP 2.

Exemptions

Nil.

4.6. IPP 5 and HPP 5: Retention and security of personal and health information

We will:

- store and dispose of personal and health information in accordance with the [General Retention and Disposal Authorities for Local Government \(GA39\)](#)
- protect information from unauthorised access, use or disclosure through access controls applied in our electronic information systems
- hold information for only as long as is required by law
- ensure that if it is necessary for information to be furnished in the provision of a service to us (i.e., through consultants and contractors), everything reasonably will be done to prevent unauthorised use or disclosure of the information including requiring the third party to dispose of information.

Exemption

I, F.

4.7. IPP 6 and HPP 6: Information about personal and health information held

An individual can find out if we hold personal or health information about them, by contacting us (see contact information on page 2).

We will:

- take all reasonable steps to enable an individual to determine whether we hold personal and/or health information about them and upon such request, we will advise of:
 - o the nature of the information
 - o the main purpose for which the information is held, and
 - o the individual's right to access the information.

A request made under IPP 6 or HPP 6 will be subject to the conditions or limitations contained in the GIPA Act. Members of the public can also apply to access information held by us under the GIPA Act.

Any person can make an application to access information held by us by completing and submitting a [GIPA application form](#).

The owner of any personal information requested under the GIPA Act will be consulted prior to any information being released and the owner of the information has the right to object to its disclosure. If we determine that there is a public interest against disclosure of the information, that information will not be released. If the owner of the information has objected and we determine that it is in the public interest to disclose the information, the owner has the right to apply for a review of our decision. Any review must be conducted prior to the release of the information.

Exemption

A, AA, C.

4.8. IPP 7 and HPP 7: Access to own information

An individual seeking to access their personal information can do so by contacting us (see contact information on page 2). We will provide individuals access to their own personal and health information without unreasonable delay or expense.

Employees wishing to access their personal information should contact the People and Culture Manager.

Exemption

A, AA, C.

4.9. IPP 8 and HPP 8: Correction or alteration of own personal and health information

Any individual who is concerned with the accuracy of their personal or health information kept by us may request for amendments to be made to that information. Any changes to personal or health information will require appropriate supporting evidence.

If we are not prepared to amend the personal or health information in accordance with the request, we may attach a statement provided by the individual to the information in question. Should we agree to do so, the statement must be attached in such a manner that is capable of being read.

If the personal or health information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have the recipients of that information notified of the amendments made by us.

Exemption

A, C.

4.10. IPP 9 and HPP 9: Accuracy of personal and health information before use of information

We will:

- prior to use or disclosure of personal or health information, take reasonable steps to ensure that the personal information is relevant, accurate, up-to-date, complete and not misleading. In doing so, we will have regard to the purpose for which the information was collected and the purpose for which it is proposed to be used.

Exemptions

Nil.

4.11. IPP 10 and HPP 10: Limits on use of personal and health information

We will not:

- use personal or health information for a purpose other than that for which it was collected unless:
 - o the individual was told at the time of collection that the information would be disclosed
 - o the individual has consented to the use of the information for that other purpose
 - o the purpose for disclosure directly relates to the purpose for which it was collected, or
 - o the use of the information for another purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

Employee information held by us may need to be used for purposes related to employee management and associated activities including safety, health and wellbeing.

Exemptions

A, B, C, E, F, G, H, J, K.

1, 2, 3.

4.12. IPP 11 and HPP 11: Limits on disclosure of personal and health information

We will not disclose personal information unless:

- the disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the individual concerned would object to the disclosure
- the individual has been made aware that this kind of information is usually disclosed, or
- we believe on reasonable grounds that disclosure is necessary to prevent or lessen a serious or imminent threat to the life of the individual concerned or another person.

We will only disclose health information under the following circumstances:

- with the consent of the individual to whom the information relates, or
- for the purpose for which the health information was collected or a directly related purpose that the individual to whom it related would expect, or
- if an exemption applies.

Exemptions

A, AA, B, C, D, E, F, G, H, I, K, L, M.

1, 2, 3.

4.13. IPP 12: Special limits on disclosure of personal information

Unless disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person, we will not disclose personal information relating to an individual's:

- ethnic or racial origin
- political opinions
- religious or philosophical beliefs
- trade union membership, or
- health or sexual activities.

We will not disclose this information to an individual or body outside New South Wales or to a Commonwealth agency unless:

- a relevant privacy law that applies to personal information concerned is in force in that jurisdiction or applies to that Commonwealth agency, or
- the disclosure is permitted under a Privacy Code of Practice.

Exemptions

A, AA, C, D, E, F, H, I, M.

4.14. HPP 12: Unique identifiers

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

** Usually a number that is assigned to an individual in conjunction with or in relation to the individual's health information for the purpose of identifying that individual. It should not include the individual's name.*

4.15. HPP 13: Anonymity

We commit to ensure that wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with us.

Exemptions

Nil.

4.16. HPP 14: Transfer of data flow

Health information will only be transferred outside New South Wales or to a Commonwealth agency if we reasonably believe:

- That the recipient of the information is subject to laws or obligations substantially similar to those imposed by the HRIP Act
- The individual consents to the transfer

- The transfer is under a contract between us and the individual
- The transfer will benefit the individual, it is impracticable to obtain the consent of the individual and if it were practicable to obtain such consent, the individual would be likely to give it
- The transfer is to lessen a serious threat to an individual's health and welfare or a serious threat to public health or public safety
- Steps have been taken to ensure that the information will not be handled inconsistently with the HRIP Act, or
- The transfer is permitted or required under any other law.

Exemptions

Nil.

4.17. HPP 15: Cross-organisational linkages

We will seek the express consent of individuals before participating in any system that links health records across more than one organisation before it will be included in the system.

Exemptions

Nil.

Part 5: Registers

5.1. Definition

Public register examples:

- Land register (section 53 of the LG Act)
- Contract registers (GIPA Act)
- Disclosure logs (GIPA Act)
- Register of returns disclosing the interest of councillors and designated persons (section 440AAB of the LG Act)
- Register of investments (GIPA Act)
- Register of delegations (GIPA Act).

We may also keep other registers or databases that are not public registers. The IPPs, HPPs, the Privacy policy, this PMP, the Privacy Code and the PPIP Act apply to those registers.

5.2. Disclosure of personal information contained in registers

Where we are responsible for keeping a public register, the register must not disclose any personal information unless we are satisfied that it is to be used for a purpose relating to the purpose of the register or in accordance with the Act under which the register is kept.

If a secondary use or disclosure of information in a register is contemplated, consent must be sought and obtained.

5.3 Application to suppress information (not public registers)

Section 739 of the LG Act.

A person may make an application to suppress certain material that is available for public inspection where the material discloses or may disclose the person's place of residence if the person considers that the disclosure would place their safety or their family safety at risk. An application must outline the risk and be verified by a statutory declaration (refer to section 739(4) of the LG Act).

5.4 Application to suppress information (public registers)

A person about whom personal information is contained (or proposed to be contained) in a public register, may make a request to have the information removed from, or not placed on the register.

If we are satisfied that the safety or wellbeing of the person would be adversely affected by not suppressing the information, we will suppress the information in accordance with the request. However, we will not suppress the information if we are of the opinion that the public interest in disclosing the information outweighs the individual interest of suppression.

Any information suppressed may still be used in the exercise of our functions, but it cannot be disclosed to other parties.

Part 6: Privacy complaints and review options

The complaints process is in three stages:

1. General complaint
2. Internal review, and
3. External review.

General complaint process

If you have a complaint about the way your personal or health information has been handled or disagree with the outcome of your application to access and/or amend your personal and health information, we encourage you first to discuss any concerns with the staff member or dealing with your information.

There are no external review rights to NSW Civil and Administrative Tribunal (NCAT) at the conclusion of a general complaint.

6.1. Internal review process

If you are not satisfied with the outcome of your general complaint, then you may apply for an internal review. Internal review is the process by which we manage formal, written privacy complaints about how we have dealt with personal information.

Click [here](#) to access the internal review application form. Although we encourage you to use the form, it is not compulsory.

You have six months from first becoming aware of the relevant conduct to apply for an internal review. Council may decline to deal with an application for internal review received after that period. Late applications will be considered on a case-by-case basis and may agree to a late application where there is evidence of hardship or another barrier preventing the application from being lodged within the legislated six-month period.

Your application will be acknowledged in writing and the acknowledgement will include an expected completion date.

We will determine whether the internal review should be handled by us alone or in consultation with another agency.

The internal review will be conducted by the Privacy Contact Officer, or by another person who:

- o was not involved in the conduct which is the subject of the complaint, and
- o is our employee or officer, and
- o is qualified to deal with the subject matter of the complaint.

The internal review will be completed within 60 days of receiving your application and we will inform you of the outcome of the review within 14 days of completing it. If the review is not completed within this time, you have the right to seek external review at the NSW Civil and Administrative Tribunal (NCAT).

We will follow the Privacy Commissioner's Internal Review Checklist (available at ipc.nsw.gov.au) and consider any relevant material submitted by you and/or the Privacy Commissioner.

A copy of the written complaint will be provided to the Privacy Commissioner.

The Privacy Commissioner may make submissions to us as part of the internal review process.

In making a decision, we may:

- o take appropriate remedial action
- o make a formal apology to you
- o implement administrative measures to prevent the conduct occurring again
- o undertake to you that the conduct will not occur again, or
- o take no further action on the matter.

You will be informed of the outcome as soon as practical following the completion of the review and within 14 days of the internal review being decided, including:

- o the findings of the review
- o the reasons for those findings
- o the action we propose to take
- o the reasons for the proposed action (or no action), and
- o your entitlement to have the findings and the reasons for the findings reviewed by NCAT.

Council must, as soon as practicable, inform the Privacy Commissioner of the internal review application, keep them informed of the progress and update them of the outcome. When we receive your application, we will provide a copy to the Privacy Commissioner.

The Privacy Commissioner must be provided the opportunity to make a submission in relation to the internal review report. This submission may be provided to the applicant. The Privacy Commissioner should receive a final copy of the report.

6.2. External review process

If you are dissatisfied with the findings of the internal review they may apply to the Administrative and Equal Opportunity Divisions of the NSW Civil and Administrative Tribunal ('NCAT') for an external review. An application must be lodged with NCAT within 28 days of receiving the report advising of the outcome of the internal review.

For more information about the external review process click [here](#).

6.3. Other options

For more information about other options for making a privacy complaint click [here](#).

Part 7: Other information

7.1 Training

Employees

Training on privacy related issues will be provided to staff on induction, with refresher training provided to all staff as required.

Public

A copy of the Privacy policy, PMP and support forms are available on our website. They can also be provided in hardcopy on request. In addition, you will see information about privacy contained in all forms and documents used by us to collect personal and health information.

7.2 Unsolicited information

Where unsolicited personal or health information is received, it will be deemed not to have been 'collected' for the purposes of IPP 1 or section 10 of the HRIP Act. However, the retention, access, use and disclosure principles will apply to such information (IPPs 5-12 and HPPs 5-15).

7.3. Public consultation processes

In accordance with the GIPA Act, when undertaking any process of public consultation where public submissions are invited by us, we will advise individuals that their submission, including any personal information in the submission, may be made publicly available. We may keep this personal information confidential on request.