Privacy Management Plan

1. Purpose of Plan

Council is committed to protecting the personal and health information that it collects from individuals and managing the information in accordance with the *Privacy and Personal Information Protection Act 1998* (**PPIPA**) and the *Health Records and Information Privacy Act 2002* (**HRIPA**).

PPIPA includes various principles which apply to Council's management of personal information, known as "Information protection principles". HRIPA includes various principles which apply to Council's management of health information, known as "Health Privacy Principles".

These "**Principles**" apply to Council's collection, storage, use, access and disclosure of personal and health information.

Section 33 of PPIPA requires all councils to prepare a Privacy Management Plan to deal with:

- the devising of policies and practices to ensure compliance by Council with PPIPA and HRIPA, in particular the Principles;
- the dissemination of those policies and practices to Council staff, contractors and councillors;
- the Council's procedures in relation to internal reviews under Part 5 of PPIPA; and
- such other matters as are considered relevant by Council in relation to privacy and the protection of Personal Information held by Council.

2. What is Personal and Health Information?

"**Personal Information**" means 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.

Examples of Personal Information held by Council, includes names, addresses and other contact information in relation to members of the public and Council staff. Also, certain employment related information of Council staff, for example, leave applications, payroll data, pecuniary interest returns and performance management plans.

Section 4(3) of PPIPA sets out the categories of information, which are not Personal Information, for example, information about an individual who has been dead for more than 30 years, and information about an individual that is contained in a publicly available publication. Information related to an individual's suitability for employment or promotion is not Personal Information.

"**Health Information**" includes Personal Information related to an individual's physical or mental health or disability, and information related to the provision of health services to an individual.

Examples of Health Information collected by Council, is information concerning Council staff, for example, medical certificates and information about medical conditions or injuries related to employment with Council.

In this Plan, a reference to "information" is a reference to both Personal and Health Information, unless otherwise specified.

3. Principles

3.1. Collection

Council collects Personal and Health information for the purpose of carrying out its lawful functions and activities, including to provide services to the community and to manage Council staff.

Examples of how information is collected include:

- DA applications (and applications for other types of approvals from Council) and submissions;
- Requests for Council services, including requests made online, over the telephone or in person;
- Reponses to surveys and public exhibition processes;
- Photographs at Council events;
- CCTV; and
- Applications for employment with Council.

Unsolicited information received by Council, is not "collected" for the purpose of this Plan. However, Council will manage such information in accordance with the Principles relating to storage, use, access and disclosure set out in this Plan.

Practices: When Council collects information, the following practices apply:

- The information must be collected for a lawful purpose that is directly related to a function or activity of Council. Council will only collect information that is reasonably necessary for that purpose and will take steps to ensure that the information collected is accurate, complete, up to date, and does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.
- Information will be collected directly from the person to whom the information relates unless:
    - someone else is authorised in writing to provide the information; or
    - If the person to whom the Personal Information relates is under 18 years of age, from a parent or guardian;
    - For Health Information, from someone else, where it would be unreasonable or impracticable to collect the Health Information, from the person to whom the information relates.

- Council will provide a **Privacy Protection Notice** where reasonable in the circumstances. The Privacy Protection Notice must advise the following:
    - That the Personal Information is being collected
    - The purposes for which the Personal Information is being collected
    - The intended recipients of the Personal Information
    - Whether the supply of Personal Information is required by law or is voluntary, and any consequences for the person if the Personal Information (or any part of it) is not provided
    - The existence of any right of access to, and correction of, the Personal Information
    - Council's name and address as the agency that is collecting and holding the Personal Information.

3.2. Retention and Security

Council takes reasonable security safeguards to protect Personal and Health Information from loss, unauthorised access, use, modification or disclosure, and against all other misuse.

Practices: The following practices apply to the retention and security of Personal and Health Information.

- Access to information will be limited to those Council staff who have a need-to-know.

- Council stores Personal and Health Information in a variety of ways including:
    - In secure physical office locations;
    - Electronic [i.e. on a server on Council's premises or a tenancy on a secure cloud network].

- Council will store information securely, keep it no longer than necessary and dispose of it appropriately in accordance with the *State Records Act 1998*. Council will protect information from unauthorised access, use, modification or disclosure.

- Council staff are subject to the requirements of the Code of Conduct in relation to the security of confidential information, including Personal and Health Information.

- Council will protect information by employing industry standard security systems based on Cyber NSW requirements for Local Councils.

- Where Council engages a third party to provide services, and the third party requires access to Personal Information and/ or Health Information, Council will take reasonable steps to ensure that the third party complies with this Plan, including ensuring that the contract includes terms requiring the protection of information in accordance with this Plan.

3.3. Use

Use refers to those occasions where Council uses the Personal Information and Health Information it holds for the performance of its functions and provide services.

Practices: The following practices apply to the use of Personal and Health Information:

- Information must be used for the purpose for which it was collected (the **Primary Purpose**).

- In limited circumstances, information may be used for another purpose (**Secondary Purpose**) where:

    - the person has given their consent for their information to used for a Secondary Purpose;
    - the Secondary Purpose is directly related to the Primary Purpose;
    - the use of the information for the Secondary Purpose is reasonably 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;
    - for the protection of public revenue; or
    - where otherwise required by law.

- Where Council engages a third party to assist Council in exercising its functions and activities, this is a use of information.

- The information must be relevant, accurate, up-to-date and not misleading before being used. The accuracy of information is checked and updated when customers contact Council's Customer Service team.

- The *Privacy Code of Practice for Local Government* provides Council with certain exemptions from the Principles regarding the use of Personal Information. The Code states that:

  Council may use personal information for a purpose other than the purpose for which it was collected where the use is for the purpose of undertaking 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.

- Health Information must only be used for the purposes set out in section 10 of Schedule 1 of HRIPA.

3.4. Access and Amendment

Practices: The following practices apply to the access and amendment of Personal and Health Information:

- Council will take reasonable steps to enable a person to ascertain whether Council holds information about them, the nature of that information, the main purpose for which the information is used and the person's entitlement to gain access to the information.

- Council must allow the person to whom the information relates to access their information without excessive delay or expense and allow them to update, correct or amend their information.

- Where a request is made to amend information; and the Council is not prepared to make that amendment, the Council will if requested, take such steps as are reasonable to attach to the information, any statement provided of the amendment sought.

How to request access to, and/or amendment of information:

- People requiring access to their Personal and Health Information held by Council can do so by filling out and submitting an Informal Information Request Form.

- Refer to Accessing Personal Information process map for further details (staff only).

- Individuals and organisations can request amendments to their contact information by filling out and submitting the following forms:
    - For individuals: Update customer details (Individuals)

    - For organisations:Update Customer Details (Organisations)

- Amendments to Health Information need to be applied for in writing, addressed to:

  CEO
  Northern Beaches Council
  PO Box 82
  MANLY NSW 1655

- The application must:
    - Provide the name and the address of the person making the request
    - Identify the health information concerned
    - Explain why the person claims the health information is inaccurate, out of date, irrelevant, incomplete or misleading.
    - If the person claims the health information is incomplete or out of date it must be accompanied by the information that the person claims is necessary to complete the health information or to bring it up to date.

- Refer to Amending Personal and Organisational Information process map for a detailed guide on how to perform this process (staff only).

3.5. Disclosure

Disclosure refers to occasions where Council releases information to a third party.

Practices: The following practices apply to the disclosure of Personal Information:

- Council will only disclose Personal Information in the following circumstances:
    - Where it has the consent of the person to whom the information relates;
    - Where the disclosure is directly related to the purpose for which the information was collected and Council has no reason to believe that the individual concerned would object to the disclosure;
    - Where the person to whom the information relates, was made aware when the information was collected (through a Privacy Protection Notice) that information of that kind is usually disclosed by Council to a person or other body;
    - Where Council reasonably believes that disclosure required to prevent a serious and imminent threat to any person's health or safety;
    - Where disclosure is required or authorised by law, for example, as part of a Court process, subpoena or notice to produce records, or pursuant to an exemption in PPIPA;
    - To a third party engaged to assist Council in exercising its functions and activities.

- Council will not disclose sensitive Personal Information unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person. Sensitive Personal Information includes information such as ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership.

- Council will not disclose Personal Information to a person or body in a jurisdiction outside of NSW or to a Commonwealth agency, except in the circumstances set out in s.19(2) of PPIPA.

- The *Privacy Code of Practice for Local Government* provides Council with certain exemptions from the Principles regarding the disclosure of Personal Information. The Code states that:

  Council may disclose personal information where the disclosure is to public sector agencies or utility providers on condition that:
  - *(i) the agency or utility provider has approached Council in writing*
  - *(ii) Council is satisfied that the information is to be used by that agency or utility provider for the proper and lawful function/s of that agency or utility provider, and*
  - *(iii) Council is satisfied that the personal information is reasonably necessary for the exercise of that agency or utility provider's function/s.*

  Where Council is requested by a potential employer, it may verify:
  - *(iv) that a current or former employee works or has worked for Council*
  - *(v) the duration of their employment, and*
  - *(vi) the position occupied during their employment.*

  This exception shall not permit Council to give an opinion as to that person's suitability to 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.

The following practices apply to the disclosure of Health Information:

- Health Information will only be disclosed in the circumstances set out in section 11 of Schedule 1 of HRIPA which include:
  - With the consent of the individual to disclose their Health Information for a purpose other than the purpose for which the information was collected;
  - For a secondary purpose which is directly related to the primary purpose for which the information was collected and the individual would reasonably expect Council to disclose their information for a secondary purpose;
  - If there a threat to the health, welfare or safety of the individual, another person or the public; or
  - For certain training and research purposes.

3.6. Other Principles relating to Health Information

- **Unique identifiers** - Council can only identify people using unique identifiers if it is reasonably necessary to carry out functions efficiently.

- **Anonymity** - Council can give people the option of receiving services from Council anonymously, where this is lawful and practicable.

- **Transfer** - Council can only transfer health information outside New South Wales in accordance with section 14, Schedule 1 of HRIPA.

- **Sharing** - Consent must be provided before health information collected by Council can be used in systems involving other organisations.

4. Public Registers

A public register is defined in section 3 of PPIPA as ". . . *a register of personal information that is required by law to be or is made, publicly available or open to public inspection*".

Personal Information contained within public registers can only be accessed if the agency is satisfied that it is to be used for the purpose for which the register exists, or a purpose provided under the relevant Act.

Council's public registers are:

- Land register
- Records of Approvals
- Register of pecuniary interest
- Rates Record
- Register of consents and approvals
- Register of building certificates
- Public register of licences held
- Record of impounding

How to request removal of Personal Information from Public Register:

- Anyone with Personal Information recorded in a public register can request their Personal Information be removed and not disclosed to the public. If Council accepts that disclosing this information could affect the person's safety or wellbeing, then it will only be disclosed if the public interest in maintaining access is greater than the personal interest in non-disclosure.
- Applications for the removal personal information from a public register must be made in writing to:

  CEO
  Northern Beaches Council
  PO Box 82
  MANLY NSW 1655

- Refer to Removal of Personal Information from a public register process map for further details (staff only).

---

5. Promoting Privacy

Council promotes compliance with PPIPA and HRIPA by:

- Making this Privacy Management Plan available to all staff and the community

- Training relevant staff in the protection and management of information - All staff are required to complete mandatory privacy training annually. New starters will be required to complete privacy training within 30 days of commencement of employment.

- Reporting any breaches to the Information and Privacy Commission NSW

6. Complaints and Rights of Review

6.1. When Should a Review Be Sought?

- Council recommends that informal attempts to resolve any privacy issues should be made prior to seeking any form of review. Only in cases where this informal approach is unsuccessful should a formal review be sought.

- Members of the public wanting to resolve any privacy issues informally, should, in the first instance, contact the Manager Information Access & Privacy.

- Staff wanting to resolve any privacy issues informally, should, in the first instance, contact the Manager Information Access & Privacy.

- Refer to the Privacy Complaints and Rights of Review process map for a detailed guide on how to perform this process (staff only).

6.2. Internal Review

- People may seek an internal review if they are of the opinion that either PPIPA or HRIPA has been breached in relation to their own personal information or the personal information of a person for whom they are an authorised representative.

- Applications for internal review must be made within six months from the date when the person became aware of the breach. Applications for an Internal Review should be made in writing to:

  CEO
  Northern Beaches Council
  PO Box 82
  MANLY NSW 1655

- The Manager Information Access & Privacy will conduct an internal review unless the review relates to the actions of the Manager Information Access & Privacy. In this instance the Executive Manager Internal Audit and Complaints Resolution will conduct the internal review.

- Applications for internal review:
  - Will be acknowledged within 5 working days
  - Will be completed within 60 calendar days.
  - Applicants will be notified of the determination of the review in writing within 14 calendar days of its completion.
  - If the applicant is not notified within 60 days of the outcome of an internal review, the applicant may then seek an external review.

6.3. Role of the Privacy Commissioner

- Council will notify the Privacy Commissioner of any internal reviews and of the progress of any internal review. The Privacy Commissioner has the right to make submissions in relation to any internal reviews.

6.4. External Review

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

- Full details of the external review process are available in Section 55 of PPIPA.

7. Other matters relevant to privacy and the protection of Personal Information

- **Appendix 1** details Council's processes for the management of CCTV.

- **Suppressing personal information**: If a person believes the disclosure of their address or contact details would place them or their family at risk, they can request their address or contact details be withheld from public view. An example of when Council may publicly display a person's address or contact details is when they have lodged a development application which is published on Council's website.

- **Mandatory Notification of Data Breach:** The Mandatory Notification of Data Breach (MNDB) scheme impacts the responsibilities of Council by requiring notifications to be provided to affected individuals and the Privacy Commissioner in the event of an eligible data breach of their Personal or Health information. For full details, please see Council's Data Breach Policy.

8. Scope and application

This Plan applies to:

- Council employees
- Consultants and contractors of Council
- Staff employed by Council-owned businesses
- Councillors

If any staff member, consultant or contractor requires advice regarding the management or handling of Personal and Health Information, in the first instance, they should seek advice from their manager.

If further assistance is required, contact the Manager Information Access & Privacy.

If a councillor requires advice regarding the management or handling of Personal and Health Information, they should seek advice from the Executive Manager Governance & Risk.

9. References and related documents

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- Privacy Code of Practice for Local Government
- Council's Code of Conduct
- Records Management OMS
- Access to Information Policy
- Data Breach Policy
- Workplace Surveillance Policy

10. Responsible Officer

Chief Information Officer

11. Review Date

28 November 2024

12. Revision History

Version	Status	Change Date	Author / Contributor	Role	Comments
1.0	Adopted	11 Sept 2019	Chris Wilson	Manager Information Management	
2.0	Reviewed	11 Sept 2021	Chris Wilson	Manager Information Management	Review and minor update
3.0	Reviewed	11 Sept 2023	Chris Wilson	Manager Information Access & Privacy	Review and update

Appendix 1

CCTV

1.0 Purpose

1.1 Council has committed as part of its *Community Safety Plan 2021 – 2026* to ensure that Council managed open spaces are safe, and that the community feels as safe as possible through the design and maintenance of community facilities and spaces.

1.2 Council incorporates the principles of *Crime Prevention through Environmental Design*, which includes surveillance, as part of all Council development and infrastructure projects, including the planning and design of open places and spaces.

1.3 Council recognises surveillance (including Closed-Circuit Television systems (CCTV)) and other forms of optical surveillance) as an effective tool in crime prevention and community safety.

1.4 The purpose of this procedure is to ensure that Council's management and operation of camera surveillance is lawful, effective and respects the privacy of individuals within our community.

1.5 A reference in this procedure to CCTV includes all other forms of camera surveillance including temporary portable security cameras, motion sensor cameras, body cameras, time lapse cameras and unmanned aerial vehicles (drones).

2.0 Principles

2.1 Council operates CCTV for the purpose of exercising its lawful functions, and only where reasonably necessary to exercise its functions.

2.2 When establishing a new CCTV operation, Council shall have due regard to the privacy of individuals, the requirements of *Privacy and Personal Information Protection Act 1998*, the *Surveillance Devices Act 2007* and the *Workplace Surveillance Act 2005*.

2.3 Council has procedures and review mechanisms in place to ensure that the information collected from its CCTV network is secure and protected from unauthorised viewing, use or disclosure.

2.4 CCTV cameras are clearly visible with appropriate signage informing individuals that the area is under surveillance and for what purpose.

2.5 Council provides clear and accessible information about CCTV on its website.

2.6 Council may consider and approve use of CCTV on its property by private entities however will not accept responsibility for the operation of CCTV or collection of information by private entities.

3.0 Council's use of CCTV

3.1 Council uses CCTV for the following purposes:

a) Enhancing public safety by identifying risk, deterring anti-social behaviour and assisting NSW Police for law enforcement purposes.

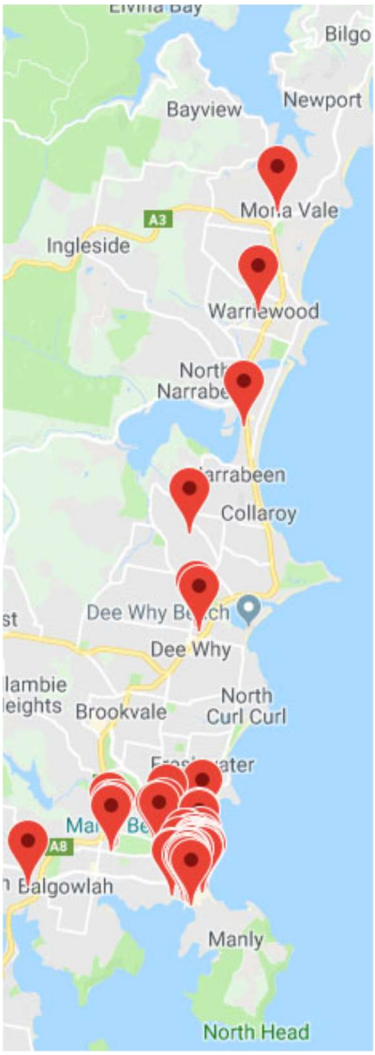
b) Monitoring our natural environment to allow for rapid response to issues such as flooding, fires and inundation during severe weather events, and to allow for monitoring of threatened species and areas of environmental sensitivity.

c) Investigation and enforcement relevant to Council legislative powers and obligations.

d) Protecting Council equipment and assets from theft and vandalism.

e) Collecting data for traffic studies and Council projects.

3.2 Council has installed CCTV at the following locations.



3.3 Council will make all reasonable attempts to ensure that CCTV operated in public places is positioned so that no other land, including residential land, is filmed unless it is not reasonably practicable to avoid filming the other land when filming the public place.

3.4 Where CCTV is installed on private land or in a vehicle, Council will ensure that obtains the consent of the owner of the land or the vehicle for installation of CCTV.

3.5 Council will ensure there is clear and accessible information about CCTV on its website, including:

a) Why Council uses CCTV and how it manages and protects information.

b) A map of the Local Government Area with the location of all of Council's cameras.

c) The contact details for CCTV enquiries.

4.0 Establishing new CCTV Operations

4.1 Before any new CCTV system is installed, a *New CCTV Operation Assessment* including a risk assessment, must be completed by the operation owner (responsible Executive Manager), and then reviewed and approved by the CEO or their delegate.

4.2 Proposed CCTV operations that may be contentious or attract public interest should include a public consultation process. The consultation requirements will be determined by the CEO or their delegate on a case by case basis depending on the scale and objectives of the operation.

4.3 Council will have regard to the NSW Government *Policy statement and guidelines for the establishment and implementation of CCTV in public places* when considering new CCTV operations.

4.4 Council will ensure that it complies with the requirements of the *Workplace Surveillance Act 2005* and Council's Workplace Surveillance Policy, when installing CCTV in places, where Council employees are at work, in accordance with that Policy.

5.0 Signage

5.1 All CCTV operated by Council will be clearly visible and have signs displayed to inform people that the area is under surveillance. Signs will be displayed near entry or access points to, or where practicable, in a prominent position within, the area of filming.

5.2 Signs will provide the following information:

a) That CCTV operates in the area

b) The purpose of the CCTV

c) Ownership of the CCTV device (being Council)

d) That footage may be disclosed to NSW Police or other law enforcement agencies

e) The hours of operation and whether it is continuous or random (eg. The footage is recorded continuously 24 hours a day, 7 days a week)

f) Contact information for enquiries.

6.0 Retention and security of CCTV footage and information

6.1 Footage and information from CCTV is stored in secure systems and retained for a prescribed period before it is deleted. The retention period will depend on the purpose of the CCTV and the operation of the CCTV system. Footage from CCTV required for the purpose of a criminal or specific investigation or court proceeding, will be kept in accordance with the *State Records Act 1998* and disposed of in accordance with the relevant disposal authority for such records made under that Act.

6.2 Access to CCTV systems, equipment and information is strictly limited to Council staff who require it to perform their duties, approved by the CEO or their delegate. Authorised staff access CCTV systems through their secure Council network login that is auditable.

6.3 Staff authorised to access CCTV systems and information will be trained and made aware of relevant procedures to ensure privacy and integrity of CCTV footage and information. Authorised staff will also be required to complete annual privacy training.

6.4 Council will ensure it has systems and processes in place to deter, detect and respond to any security breaches.

6.5 Where a third party engaged by Council to provide goods or services requires access to CCTV footage, Council will, using reasonable endeavours, ensure that the contract or terms of engagement require compliance by the third party with this procedure and Council's Privacy Management Plan.

7.0 Disclosure of Information

7.1 Some CCTV cameras broadcast a live stream to the Police Area Commands. Recorded images are also made available to the NSW Police for law enforcement purposes. The NSW Police lodge requests for footage using established protocols.

7.2 The release of footage to members of the public is governed by the requirements of the *Government Information (Public Access) Act 2009* and *Privacy and Personal Information Protection Act 1998*.

7.3 Any requests to access information must be made in line with Council's information access protocols visit https://www.northernbeaches.nsw.gov.au/council/information-access.

8.0 Audit, review and evaluation

8.1 CCTV operations will be reviewed as required. The review may consider the effectiveness of a camera and whether it achieves its purpose, location and condition of cameras and signage and the necessity of the continued operation of the camera.

8.2 Council will ensure CCTV is scheduled as part of Council's audit program on a regular basis.

9.0 Complaints

9.1 Complaints about CCTV will be managed in accordance with Council's Complaints Management Policy.

9.2 Complaints must be made in writing and submitted though the complaints form online or sent to:

Email:
Council@northernbeaches.nsw.gov.au

Post:
Complaints
Northern Beaches Council
PO Box 82
MANLY NSW 1655

10.0 References and related documents

- NSW Government policy statement and guidelines for the establishment and implementation of closed circuit television (CCTV) in public places
- Workplace Surveillance Policy (Operational)
- Complaints Management Policy
- Privacy Management Plan (Operational)
- Northern Beaches Council Code of Conduct
- Workplace Surveillance Act NSW 2005
- Government Information (Public Access) Act 2009
- Privacy and Personal Information Protection Act NSW 1998
- The NSW Local Government Act 1993
- State Records Act 1998
- Civil Aviation Safety Regulations 1998