Privacy Management Plan

1 Purpose of Plan

The *Privacy and Personal Information Protection Act 1998* (PPIPA) and the *Health Records and Information Privacy Act 2002* (HRIPA) provide for the protection of personal and health information and the protection of privacy of individuals. Section 33 of PPIPA requires all councils to prepare a Privacy Management Plan to deal with:

- Ensuring compliance with the requirements of PPIPA and HRIPA
- The dissemination of compliance requirements to all who are required to comply.

Council also has a Privacy Policy that explains Council's commitment to privacy to our community. The purpose of this Plan is to guide council officers in applying the principles of privacy to their decision making in the workplace.

2 Principles

2.1 Collecting Personal and Health Information

Northern Beaches Council collects personal information for business purposes in order to provide services to the community. Examples of how information is collected include, but are not limited to:

- Rates records
- DA applications and submissions
- Online forms for services

Council also holds personal and health information relating to employees, such as:

- Leave and payroll data
- Personal contact information
- Performance management plans
- Pecuniary interest returns
- Health information such as medical certificates.

When Council collects personal and health information, the following must apply:

- It is being collected for a lawful purpose
- It is being collected directly from the person to whom the information relates or from someone authorised to provide the information (such as a parent or guardian) if the person is under 18 years of age.
- The person to whom the information relates must be advised the information is being collected, why it is being collected, and who will be storing and using it.
- The personal information must be relevant, accurate, complete, up-to-date and not excessive.
- When collecting personal information, the person from whom the information is being collected must be informed if the information is required by law or is voluntary and if there are any consequences to not providing it.

2.1.1 Privacy Protection Notice

Council must include a Privacy Protection Notice on all forms and correspondence that result in the collection of personal information to ensure that people are aware that their personal information is being collected. The Privacy Protection Notice must advise the following:

- That the information is being collected
- The purposes for which the information is being collected
- The intended recipients of the information
- Whether the supply of personal information is required by law or is voluntary, and any consequences for the person if the information (or any part of it) is not provided
- The existence of any right of access to, and correction of, the information
- Council's name and address as the agency that is collecting and holding the information.

2.2 Personal and Health Information about Children

Northern Beaches Council collects personal and health information about children and youths (and their parent/guardian) to whom we provide services, for example, children who attend one of Council's Long Day Care Centres. Whether a child or youth has the capacity to make his or her own privacy decisions will be assessed on a case by case basis, having regard to factors such as their age and circumstances. In general, a person over 18 years will have the capacity to make his or her own privacy decisions.

For children who are under 18 years old, or who otherwise do not have capacity to make these decisions, or where we cannot make an assessment of their capacity, Council will manage requests for access, consent and notices in relation to personal and health information via the parent or guardian. Council will treat consent given by a parent or guardian as consent given on behalf of the child.

2.3 Storing Personal and Health Information

Council must store personal and health information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

2.4 Using Personal and Health Information

When using personal and health information, it must be used for the purpose for which it was collected, or a directly related purpose that the person would expect. Otherwise, the consent of the person to whom the information relates is required.

The information must be relevant, accurate and up-to-date before being used.

2.5 Accessing Personal and Health Information

Council must allow the person to whom the information relates to access their personal and health information without excessive delay or expense and allow them to update, correct or amend their personal and health information. Council must also explain why it is being collected and used.

2.6 Limitations on Access and Amendments to Personal and Health Information

A person is only entitled to access their own personal and health information. The only exceptions are:

- If the person to whom the information relates has advised Council in writing to provide access to another person
- If the person to whom the personal and health information relates is incapable of accessing the information themselves for reasons such as age, injury, illness, physical or mental impairment and another person has been authorised to do so

- If a serious or imminent threat to life or serious health and safety can be avoided through the release of personal and health information.

2.7 Disclosing Personal and Health Information

Council can not disclose sensitive personal and health information without consent. This includes information such as ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership**.**

Other personal and health information can only be disclosed in limited circumstances. Disclosure requires consent unless the person was advised that it would be disclosed at the time of collection or if the disclosure is directly related to the purpose for which it was collected and it could be assumed the person would not object or if the disclosure is required to prevent a serious and imminent threat to any person's health or safety.

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.

2.8 Additional Privacy Considerations with Health Information

There are additional considerations applying specifically to health information. These are:

- 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 the Health Privacy Principles that form part of HRIPA.

- Sharing

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

3 Operational Management Standards

3.1 Intended Audience

This Plan applies to:

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

3.2 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.

Northern Beaches 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

3.3 Removal of Personal Information

Anyone with personal information recorded in a public register can request their personal information be removed. 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 process map for further details.

3.4 Accessing Personal and Health 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.

3.5 Amending Personal and Health Information

Individuals and organisations can request amendments to their personal information or to organisations by filling out and submitting the following forms:

- For individuals:

Update customer details (Individuals)

- For organisations:

Update Customer Details (Organisations)

Access will be provided and amendments will be made without charge.

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.

3.6 Who to Contact for Assistance or Advice Regarding Personal Information

If any staff member requires advice regarding the management or handling of personal information, in the first instance, they should seek advice from their manager.

If further assistance is required, contact the Manager Information Management.

3.7 Complaints and Rights of Review

3.7.1 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 Management will conduct an internal review unless the review relates to the actions of the Manager Information Management. In this instance the Executive Manager Internal Audit and Review 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.

3.7.2 Role of the Privacy Commissioner

Northern Beaches 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.

3.7.3 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.

3.7.4 When Should a Review Be Sought?

Northern Beaches Council recommends that informal attempts to resolve any privacy issues should be attempted 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 Management.

Staff wanting to resolve any privacy issues informally, should, in the first instance, contact the Manager Information Management.

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

3.8 Promoting Privacy

Northern Beaches Council promotes compliance with PPIPA and HRIPA by:

- Making this Privacy Management Plan available to all staff
- Training relevant staff in the protection and management of personal information
- Reporting any breaches to the Office of the Information and Privacy Commission.

3.9 Privacy Training

Some staff within the organisation occupy positions that require a greater understanding of privacy and personal information than most. These include:

- Customer Service staff
- Information Management staff
- Executive Leadership Team members
- Any staff that have a significant amount of contact with members of the public.

4 Authorisation

This Plan was adopted by the CET on 11 September 2019

It is effective from 11 September 2019

Last reviewed on 29 September 2021

It is due for review by 29 September 2022

5 Amendments

This Plan was last amended on 29 September 2021

6 Who is Responsible for implementing this Plan?

Chief Information Officer

7 Document Owner

Director Workforce & Technology

8 Related Council Documents

Records Management OMS

Access to Information Policy

9 Legislation and References

a) Government Information (Public Access) Act 2009 (NSW)

b) Privacy and Personal Information Protection Act

c) Privacy Act 1988 (Commonwealth)

d) Privacy Code of Practice for Local Government

10 Definitions

Personal Information

Information or an opinion about a person whose identity is apparent or can be reasonably ascertained from the information or opinion. This information can be on a database and does not necessarily have to be recorded in written form.

Personal information does not include information about a person that is contained in a publicly available publication.

Health Information

Information or an opinion about:

- The physical or mental health or a disability of a person
- An person's express wishes about the future provision of health services to him or her
- A health service provided, or to be provided, to a person.
- Other personal information collected:

  To provide, or in providing, a health service

  In connection with the donation, or intended donation, of a person's body parts, organs or body substances

  Regarding genetic information about a person arising from a health service provided to the person in a form that is or could be predictive of the health (at any time) of the person or of a genetic relative of the person.

Appendix 1

Management of credit card information

Northern Beaches Council will act in accordance with the *Payment Card Industry- Data Security Standard (PCI-DSS).*

Northern Beaches Council handles cardholder data for business purposes in order to take payment for services provided to the community.

Cardholder data will only be used for the transaction at the time the card data is presented and not stored for use at a later time.

Any payments that need to be processed on a recurring/regular basis must have been assessed by the relevantauthority and approved as being PCI Compliant. Rules against which the process will be assessed include but are not limited to the following:

- There is a genuine business requirement
- Only the first 6 and last 4 digits of any card number are stored without encryption/redaction
- Sensitive authentication data e.g. CCV/CVV number is not stored
- The data is only stored for as long as there is a valid business purpose

All wireless networks must be protected using secure data encryption that meets PCI-DSS standards.

When receiving cardholder details, the following applies to each format:

Phone

- Calls cannot be recorded
- Cardholder data must be directly entered into the payment terminal during the call
- The cardholder needs to stay on the phone until the transaction has been completed

Email

- Cardholder data is not to be transmitted via email
- Forms that can hold payment information should not offer email as an option for lodging the form and if received in this way, not processed. The cardholder should be advised of this and the email destroyed
- The above also applies to Council's e-fax as it converts the fax to an email

Fax

- In order to take payments via fax, a physical fax machine must be used.

Post

- Cardholder data received in hard-copy needs to be kept securely, processed as soon as possible and destroyed in accordance with the correct standards.

Data Access

Access to cardholder data and system components should be limited and restricted to only those individuals whose job requires such access.

Data Storage

Bank details and cardholder data are only stored if there is a reasonable business justification

Cardholder data should be masked and rendered unreadable whenever displayed or stored, e.g. after the payment is processed and before the form is shredded.

Data Retention

Council is obliged to maintain records in line with the *NSW State Records Act 1998*. According to GA 39 section 12.1.8, the following applies to cardholder information and section 12.1.9, payment information:

12.1.8

Records containing sensitive cardholder authentication data captured as part of an electronic financial transaction.

Note: Management of these records should be in accordance with the Payment Card Industry - Data Security Standard (PCI-DSS).

Retain until transaction completed, then destroy.

12.1.9

Records containing cardholder data captured as part of an electronic financial transaction including information printed, processed, transmitted or stored in any form on a payment.

Note: Management of these records should be in accordance with the Payment Card Industry - Data Security Standard (PCI-DSS).

Retain minimum of 3 months after last business, legal and/or regulatory action, then destroy.

Data Disposal

A programmatic (automatic) process will be executed on cardholder data systems nightly to remove all confidential or sensitive data that exceeds business retention requirements.

Regarding paper containing cardholder data, a review must be conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed retention policy requirements.

Payment Terminal Device Inspections

Periodically inspect payment terminals and devices to check compliance with the PCI DSS and to detect tampering or substitution, for example, check serial number, condition of tamper proof seals, unexpected cables/attachments, broken/changed casing, addition of card skimmer to devices.

Appendix 2

CCTV

Northern Beaches Council has installed CCTV cameras at various locations throughout the LGA (see map below for current camera locations).

The cameras in the CCTV network have been installed as part of a plan to deal with issues include but are not limited to:

- The monitoring of behaviour in Manly Corso and other locations
- Assisting NSW Police to identify people involved in criminal activity
- Creating an increased sense of safety in the community.

Some of the cameras broadcast a live stream to Manly Police Station. Recorded images are also made available to NSW Police for law enforcement purposes.

CCTV collection and use will:

- Occur with due regard to applicable law
- Be operated with due regard to the privacy of individual members of the public.

Council's CCTV program is governed by protocols that ensure:

- Access to equipment that holds CCTV footage is strictly controlled and password protected
- NSW Police lodge requests for footage using established protocols
- The release of footage to the community is governed by the established Government Information (Public Access) Act 2009 and/or Privacy and Personal Information Protection Act 1998 processes.

Adequate signage is to be put in place to ensure the public is aware of the camera's proximity to them, the contact details for the ownership of the scheme, the purpose of the scheme, and hours of operation.

NB: The *Privacy and Personal Information Protection Amendment (CCTV) Regulation 2013* provides Council with exemptions from certain provisions of the *Privacy and Personal Information Protection Act 1998* relating to the collection of personal information, by using a CCTV camera installed for the purpose of filming a public place, and the disclosure to the NSW Police Force of that information by way of live transmission.

Mobile CCTV

In addition to the networked CCTV system, Council employs portable cameras that can be relocated to various positions or temporarily placed in a position for a specified time for surveillance.

Council officers and volunteers can use Mobile CCTV cameras provided that they comply with the relevant legislation.

Signage must be put in place with mobile cameras. The signage requirements are the same as for fixed cameras.

Appendix 3

Workplace Surveillance

Northern Beaches Council will comply with the Workplace Surveillance Act 2005.

Northern Beaches Council conducts workplace surveillance in the following ways:

- CCTV

  CCTV cameras may be used for operational, security or safety reasons on Council facilities. When used, cameras will be visible and appropriate signage will be in place to advise people that surveillance is being carried out. When new cameras are introduced, staff will be notified 14 days prior to commencement. When the camera is to be used for safety purposes such as remote sites or to monitor hazardous activities, staff will consult these employees prior to the commencement of surveillance.

- Computer surveillance

  Any data, information or intellectual property that is created in the course of staff performing their work is considered to be Council property. To ensure it is being managed effectively, this data, information and intellectual property and/or metadata relating to these may be accessed and monitored. This includes computer, email and internet usage. Whilst IT resources are provided for business purposes, reasonable personal use is permitted.

- Tracking surveillance

  Council tracks its fleet and IT equipment to ensure it is being used appropriately and to track its whereabouts for operational, security and safety reasons. Visible signs will be installed in vehicles fitted with tracking devices.

Surveillance data will not be used to initiate investigations, although it may form part of the evidence used in investigations for disciplinary purposes. Cases where this data may be used are in connection with suspected corruption, maladministration, misuse of resources, threats of violence or substantial damage to property in accordance with section 18 of the Workplace Surveillance Act.

Covert surveillance will only be carried out in cases where there is already the belief that an employee or group of employees is engaging in unlawful activity within the workplace. This requires a covert surveillance authority to be issued by a magistrate. Covert surveillance will always be carried out in accordance with the Workplace Surveillance Act.

Appendix 4

Use of drone technology

Council will comply with CASA regulations in the use of drones.

Council will not operate drones over private property without the consent of the property owner.

Approval to use a drone must be in writing and issued by a Director or the CEO.

All data collected or recorded by Council managed drones, including geospatial data, is owned by Council and is subject to Council's Privacy Policy, Privacy Management Plan and the State Records Act.

Data is collected only for a specific purpose in support of a Council function. Data gathered will be stored in Council's Electronic Document Management System, enabling it to be used for operational and/or regulatory purposes.

Any personal information collected using drones will be destroyed or de-identified when it is no longer needed for the purpose for which it was collected.

Council is subject to the *Privacy and Personal Information Protection Act 1998* when using drones to collect data.