# North Sydney Council
# Privacy Management Plan

**Adopted by North Sydney Council: (the General Manager has authorised this Privacy Management Plan under delegated authority): 13 July 2021**
**Date sent to the New South Wales Privacy Commissioner: 13 July 2021**
**Updated in response to feedback from the NSW Privacy Commissioner: 24 September 2021**
**Next Review to be completed no later than: 13 July 2023**

# Contents

# 1. Privacy Management Plan overview

## 1.1 Purpose

1.1.1 The purpose of this Privacy Management Plan (**PMP**) is to explain how North Sydney Council (**Council**, **we**, **our**, **us**) manages personal and health information about individuals (**you**, **your**), and our strategies for complying with the:

(a) *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**); and

(b) *Health Record and Information Privacy Act 2002* (NSW) (**HRIP Act**).

1.1.2 This PMP sets out the functions and activities of Council and our privacy obligations in relation to those functions and activities. The PMP also includes information:

(a) on how we handle and store personal and health information, including what information is covered by the PPIP Act and HRIP Act, and any exemptions that we may rely on relating to our obligations;

(b) about who to contact if you have questions about the information collected and held by Council;

(c) on how to access and amend your information; and

(d) about what to do if you believe that Council has breached the PPIP or HRIP Acts.

## 1.2 What this PMP covers

1.2.1 Council is considered a 'public sector agency', as defined in section 3 of the PPIP Act.

1.2.2 Accordingly, Council is required to have a PMP under section 33 of the PPIP Act, which must include information on:

(a) how Council develops policies and practices to ensure compliance with the PPIP Act and the HRIP Act;

(b) how Council disseminates these policies and practices within the agency, and trains our staff in their use of the PMP;

(c) Council's internal review procedure; and

(d) anything else Council considers relevant to the PMP in relation to privacy, and the personal and health information it holds.

1.2.3 This PMP meets the requirements for privacy management plans under section 33 of the PPIP Act, and demonstrates to members of the public, including Council constituents, how Council meets its privacy obligations under the PPIP Act and the HRIP Act.

1.2.4 It also acts as a key reference for Council's employees, contractors, service providers and elected representatives (**Councillors**) to:

(a) explain how Council complies with the requirements of the PPIP Act and the HRIP Act; and

(b) prompt employees, contractors, service providers and Councillors to seek further advice where they are unsure about applicable privacy requirements.

### 1.3 Background to, and approach to reviewing and updating, this PMP

1.3.1 Council undertook a significant review in 2021 to create this current version of the PMP. The process involved to create this current version of the PMP included:

(a) a comprehensive privacy review survey involving key stakeholders across Council's divisions and key departments who handle personal information to ensure that the information captured in this PMP is current and up-to-date at the time of publication;

(b) further consultation with internal stakeholders at Council, including face-to-face meetings, and seeking feedback on working drafts of this PMP;

(c) using resources provided by the Information and Privacy Commission NSW (**IPC**), the independent statutory authority that administers legislation dealing with privacy, and access to government held information in New South Wales (**NSW**);

(d) considering emerging 'good practice' privacy management plans implemented by other NSW public sector agencies and the IPC itself as a quality control benchmark; and

(e) using the IPC's 'Checklist - Privacy Management Plans' tool to assess the content of the PMP once it was prepared, to ensure the PMP addressed all of the section 33 requirements of the PPIP Act.

1.3.2 This PMP will be reviewed and updated every 2 years using a similar process as outlined above (which will be updated and amended as required).

1.3.3 However, if there are major changes to the ways in which we handle personal information, or to the mandatory matters which must be covered in this PMP, Council may update a relevant section of this PMP at the relevant time and prior to the next scheduled 2 year review process.

1.3.4 As soon as practicable after this PMP is finalised, Council will provide a copy of this PMP to the IPC for its consideration. Council will consider and incorporate feedback received from the IPC when conducting its next scheduled review of this PMP.

1.3.5 In addition, Council welcomes feedback on this PMP from its other stakeholders, including the public. Any feedback we receive will be considered as part of our review process (set out in this section 1.3 of this PMP). Feedback must be provided in writing, and addressed to the Privacy Contact Officer (see details in section 2.5 of this PMP).

## 2. Introduction

### 2.1 About Council and its organisational structure

2.1.1 Council's primary responsibilities are mainly under the *Local Government Act 1993* (NSW) (**Local Government Act**).

2.1.2 However, Council also has responsibilities under other Commonwealth and NSW laws, including the *Environmental Planning and Assessment Act 1979* (NSW)

(**Environment Planning and Assessment Act**), the *Public Health Act 2010* (NSW), the *Companion Animals Act 1998* (NSW), the *State Records Act 1998* (NSW), and the *Government Information (Public Access) Act 2009* (NSW), and the Commonwealth privacy act, *Privacy Act 1988* (Cth) (**Commonwealth Privacy Act**).

2.1.3 Council is consisted of divisions and departments within them, as follows:

| Division | Department |
|---|---|
| **City Strategy Division** | Administrative Services |
| | Development Services |
| | Environmental and Building Compliance |
| | Strategic Planning (Land Use) |
| | Ranger and Parking Services |
| **Community and Library Services Division** | Community Development |
| | Library Services. |
| **Corporate Services Division** | Communications and Events |
| | Customer Services |
| | Document Management Services |
| | Financial Services |
| | Human Resources |
| | Information Technology |
| | Contracts |
| | Procurement Services |
| **Engineering and Property Services Division** | Asset Management |
| | Engineering Infrastructure |
| | Project Management |
| | Property Assets |
| | Traffic and Transport Operations |
| | Works Engineering |
| **Open Space and Environmental Services Division** | Environmental Services |
| | Landscape Planning and Design |
| | North Sydney Oval and Mollie Dive Function Centre |
| | North Sydney Olympic Pool |
| | Parks and Reserves |
| **Governance Division** | Legal Services |
| | Governance and Committee Services |
| | Corporate Planning and Consultation |
| | Risk and WHS) |

2.1.4 Council provides a range of services to our local community via the above divisions, and is responsible for issues that affect people's daily lives.

2.1.5 The functions and activities of Council include the following:

(a) providing a representative, informed and responsible decision making body;

(b) developing the local community and its resources;

(c) maintaining libraries, community centres, and halls;

(d) maintaining recreation facilities, such as public swimming pools and sporting fields;

(e) maintaining infrastructure, such as roads, bridges, boat ramps, skate parks, public toilets and picnic areas;

(f) providing environmental and public health services;

(g) controlling companion animals;

(h) planning and development services; and

(i) providing services for specific groups in the community, such as children, young people, older people, people with disabilities, Indigenous people and people from culturally and linguistically diverse backgrounds.

2.1.6 Council also has elected representatives, who are Councillors (one of whom is the Mayor).

2.1.7 In addition to providing services to constituents and the community, Council provides services to Councillors to facilitate the performance of their role including making event and travel bookings, processing reimbursements and other administrative support.

## 2.2 Developing privacy-related policies and practices

2.2.1 Council's privacy-related policies and practices are developed by:

(a) examining changes in legislation, policy and IPC guidance for their impacts on Council's privacy management;

(b) conducting regular reviews of its privacy policies; and

(c) considering the privacy implications of changes to policies, systems and the ways in which we handle personal and health information.

2.2.2 A list of all our current and formally adopted policies is available on Council's website.

2.2.3 Council also develops privacy-related policies and practices through:

(a) **consulting with the general public**, including making draft policies publicly available, and inviting and considering submissions (which occurred for our Closed Circuit Television Policy);

(b) **internal working groups**, such as our InfoSec Working Group (which at the time of publishing this PMP is currently developing a range of relevant

policies and procedures relating to cybersecurity and incident response, which have privacy implications); and

(c) **consulting with external subject matter experts**, such as consultants, forensic and security experts, privacy and local government lawyers and other advisors on a range of issues, where appropriate (for example, in relation to records management, cyber security, and privacy and local government compliance).

2.2.4 Council is currently in the process of undertaking a major recordkeeping review (**Recordkeeping Review**), working closely with an external consultant. This Recordkeeping Review has involved a comprehensive review of Council's records and information management governance, practices, and systems across Council.

2.2.5 As a result of this Recordkeeping Review, Council is in the process of updating a number of its records-related policies and practices that have been identified as areas for improvement. Once implemented, these recommendations will also impact privacy and how we handle personal and health information (by improving our approach and information handling processes).

2.2.6 Our PMP will be updated as the recommendations from this Recordkeeping Review are implemented, and new policies and procedures are approved and introduced more generally.

## 2.3 Disseminating the PMP within Council

2.3.1 Council promotes the PMP and awareness of privacy obligations by taking the following actions:

(a) making the PMP publicly available on Council's website, and available to staff via Council's electronic document management system;

(b) ensuring that the PMP is clear and easy to understand, by drafting it using plain English;

(c) providing annual privacy training to employees and Councillors;

(d) ensuring that new employees and Councillors receive briefings on privacy policies and issues at induction and other relevant times; and

(e) communicating regularly with employees and Councillors about privacy matters through emails, team meetings, and posters.

2.3.2 All Councillors must also complete training in topics, including meeting procedures, planning legislation (including privacy compliance), financial issues, codes of conduct, and conflicts of interest.

2.3.3 When employees, contractors, service providers or Councillors have questions about the PMP or their privacy obligations, they are encouraged (including through this PMP) to consult with Council's Privacy Contact Officer.

## 2.4 Responsibilities of employees, Councillors, contractors, and service providers

2.4.1 All employees, Councillors, contractors, and service providers of Council are required to comply with the PPIP Act and HRIP Act (for the purposes of this section 2.4, the **Acts**), including any applicable privacy principles contained in both those Acts.

2.4.2 If these privacy principles are breached, Council may face reputational risk, loss of customer or stakeholder trust, and financial costs (including compensation).

2.4.3 Both Acts also contain criminal offence provisions applicable to Council's employees, Councillors, contractors and service providers who use or disclose personal information or health information otherwise than in connection with lawful exercise of official functions.

2.4.4 This PMP is intended to assist Council's employees, Councillors, contractors, and service providers to understand, and assist them in complying with, their obligations under those Acts.

2.4.5 If Council's employees, Councillors, contractors or service providers feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice from the Privacy Contact Officer (see section 2.5 below for the relevant contact details).

2.4.6 Council's employees, Councillors, contractors, or service providers who are suspected of conduct which would breach the privacy principles or the criminal provisions specified in the Acts may be disciplined for a breach of Council's Code of Conduct.

2.4.7 Suspected criminal conduct may result in dismissal and/or referral to NSW Police.

2.4.8 For example, under sections 62-68 of PPIP Act and sections 68-70 of the HRIP Act, it is an offence (punishable by up to two years' imprisonment, an $11,000 fine, or both) for Council (including its employees, Councillors, and contracts) to:

(a) intentionally disclose or use personal or health information accessed in the course of doing your job for an unauthorised purpose;

(b) offer to supply personal or health information for an unauthorised purpose;

(c) attempt by threat, intimidation, etc., to dissuade a person from making or pursuing a request for health information, a complaint to the NSW Privacy Commissioner (**Privacy Commissioner**) about health information, or an internal review under the HRIP Act, or

(d) hinder the Privacy Commissioner or member of their staff from doing their job.

2.4.9 It is also a criminal offence, punishable by up to two years' imprisonment, for any person to cause any unauthorised access to or modification of restricted data held in a computer (see section 308H of the *Crimes Act 1900* (NSW)).

**IMPORTANT NOTE**
It is also a criminal offence, punishable by up to two years' imprisonment, an $11,000 fine, or both, for any person employed or engaged by Council (including former employees and contractors) to intentionally use, disclose or offer to supply any personal information or health information about another person, to which the employee or contractor has or had access in the exercise of their official functions, except in connection with the lawful exercise of his or her official functions.

### 2.5 Privacy Contact Officer for Council

2.5.1 For further information about this PMP, the personal and health information that Council holds, or any other privacy concerns, please contact Council's Privacy Contact Officer, at:

**Email:** council@northsydney.nsw.gov.au

**Phone:** 02 9936 8100

**Mail:** North Sydney Council, PO Box 12, North Sydney NSW 2059

**Visit:** 200 Miller Street, North Sydney NSW 2060

**IMPORTANT NOTE**
Applications for internal review **must be in writing**. Therefore these applications must be provided to the Privacy Contact Officer by post, email or delivery to Council's offices. Please see section 8.2 for further information.

### 2.6 Responsibilities of the Privacy Contact Officer

2.6.1 The Privacy Contact Officer is responsible for ensuring that Council complies with its obligations under the PPIP and HRIP Acts.

2.6.2 The functions of the Privacy Contact Officer include:

(a) reviewing and updating the PMP;

(b) creating, updating and publishing any guidance material available to Council employees and councillors;

(c) recommending controls to manage privacy risks;

(d) responding to privacy complaints and incidents;

(e) responding to applications for internal review and conducting internal reviews;

(f) overseeing the development of training and awareness activities to Council employees and Councillors; and

(g) being available to answer any questions employees or Councillors have about their privacy obligations.

2.6.3 The Privacy Contact Officer is also available to answer any questions from the public about how Council manages personal and health information.

## 3. Types of information collected and held by Council

Council collects and holds both personal information and health information.

### 3.1 Personal and health information

3.1.1 Personal information is defined in section 4 of the PPIP Act. It means information or an opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. Personal information can include a person's name, address, details about their family life, financial information, and photos.

3.1.2 Health information is defined in section 6 of the HRIP Act and includes information or an opinion about an individual's:

(a) physical or mental health or a disability;

(b) express wishes about the future provision of health services to him or her;

(c) health service provided or to be provided to him or her; or

(d) health care identifiers.

3.1.3 Due to the number of different roles that Council plays, the type of personal and health information held is also diverse.

3.1.4 There are three main categories of personal and health information that we collect, hold or have access to. These are:

(a) personal and health information about members of the public, including constituents and other members of the public (**customer records**);

(b) personal and health information about our staff (**employee and contractor records**); and

(c) personal and health information about our Councillors (**Councillor records**).

### 3.2 Customer records

3.2.1 These are records relating to our constituents, customers and other stakeholders we deal with when performing our functions and activities as a local council and providing our services, including those described in section 2 of this PMP.

3.2.2 Council interacts with customers through various channels, which means that Council may collect personal and health information from you when you interact with us. This includes:

(a) **in person** at our Customer Service Centre located at Council, at venues we operate or at events and community engagement activities we run, and via staff performing their duties in Council's local government area (such as our parks staff);

(b) **by phone** (general inquiries, and department and division-specific inquiries); and

(c) **online** through our website (including through 'Your Say North Sydney') or through your interaction with our social media channels and other digital facilities, including to submit applications or making general enquiries.

3.2.3 Council generally collects and holds the following information in its customer records:

(a) names, gender, age and date of birth;

(b) contact details, such as phone numbers, residential and email addresses;

(c) opinions, feedback and survey results;

(d) health conditions;

(e) family relationships;

(f) financial information, such as credit card details and bank account details;

(g) drivers licence and vehicle registration information;

(h) copies of identity documents, where we need to verify your identity;

(i) images, such as photos and videos (which may be captured by our staff at events or functions or via the surveillance technology we use); and

(j) work and education details.

**3.3 Employee and contractor information**

3.3.1 The types of personal and health information collected and held by Council about employees and contractors include:

(a) identity, demographic and contact information (such as name, address, and telephone numbers);

(b) email address, date of birth, gender, and signature;

(c) payroll, attendance and leave records;

(d) bank account details and financial records;

(e) performance management and evaluation records;

(f) referee reports;

(g) redundancy and termination decisions;

(h) workers' compensation records;

(i) work health and safety records;

(j) medical assessments, records, and certificates; and

(k) records of gender, ethnicity, and disability of employees for equal employment opportunity reporting purposes.

**3.4 Councillor records**

3.4.1 Council also collects and holds information about Councillors in order to perform its functions and activities, which includes:

(a) identity, demographic and contact data such as name, address, and telephone numbers;

(b) email address, date of birth, gender, and signature;

(c) bank account details and financial records (for processing reimbursements);

(d) reports and records relating to training and education required to be undertaken by Councillors as part of their roles and duties;

(e) reports and records relating to the conduct investigations, disciplinary action, investigations or legal proceedings, including status updates relating to legal proceedings and the outcome of legal proceedings;

(f) photographs, videos and audio recordings of Councillors conducting activities related to Council (including attendance at meetings and Council events);

(g) a broad range of records relating to each Councillor roles and duties (such as copies of agendas, committee attendance, records of meetings, meeting transcripts, internal and external reports);

(h) records in relation to Council providing administrative services to Councillors (such as records relating to travel and other expenses claimed by Councillors for the purpose of processing reimbursements); and

(i) other information which Councillors' may provide to Council from time-to-time and which Council may lawfully collect and hold; and

(j) records of gender, ethnicity, and disability of Councillors for equal reporting purposes or to assist with specific individual requirements.

### 3.5 What is <u>not</u> personal information?

3.5.1 The PPIP Act states that certain types of information do not fall within the definition of personal information (see section 4(3) of the PPIP Act). These include:

(a) information about a person who has been dead for more than 30 years;

(b) information about an individual that is contained in a publicly available publication (for example where we lawfully publish materials or records on our website, or personal information that is published in the newspaper by a media outlet); and

(c) information or an opinion about an individual's suitability for appointment or employment as a public sector official.

3.5.2 The *Privacy and Personal Information Protection Regulation 2019* lists other information that is not personal information relevant to Council's activities and functions. This includes information about an individual contained one of the following:

(a) a document in a library, art gallery or museum;

(b) state records, that are available for public inspection, and under the control of the NSW State Archives and Records; and

(c) archives (within the meaning of the *Copyright Act 1968* (Cth)).

## 4. How the Privacy Principles apply

### 4.1 The Privacy Principles

4.1.1 The Information Privacy Principles and Health Privacy Principles (**Privacy Principles**) outline Council's obligations under both the PPIP and HRIP Acts in relation to how we collect, use, store and disclose personal and health information. This section sets out how we manage information in compliance with these Privacy Principles, as well as common exemptions that Council relies on.

### 4.2 Exemptions to the Privacy Principles

4.2.1 The obligations under the PPIP Act and the HRIP Act only apply if information falls within the definitions of "personal information" and "health information" (as relevant). Accordingly, the requirements and obligations in the PPIP Act (including the IPPs) for example, do not apply to any information that does not fall within the definition of personal information (e.g., the IPPs will not apply to information that is about an individual that is contained in a publicly available publication – see further exclusions above in section 3.5.1 above).

4.2.2 Under the PPIP Act and the HRIP Act, in certain circumstances agencies may be exempted from complying with their obligations in relation to personal and health information under the Acts (including in respect of specific IPPs and HPPs).

4.2.3 Some of the key exemptions under the PPIP Act and the HRIP Act that Council may rely on include:

(a) for law enforcement and investigative purposes (for example, to investigate suspected fraud);

(b) for the purposes of research that are in the public interest;

(c) for the purposes of exchanging information between public sector agencies (for example, to enable inquires to be referred between agencies); and

(d) if another law authorises, requires, implies, or reasonably contemplates the use or disclosure (for example, laws relating to local councils, including the Local Government Act (e.g., this Act mandates that Council must prepare and publish certain reports put before Council (and associated committees within Council)).

### 4.3 Collection of personal information (IPPs 1,2, 4; HPPs 1, 2, 3)

4.3.1 Council collects and receives personal and health information in a variety of ways in order to fulfill our functions and provide services to the community. Information may be collected in writing, in person, over the phone or via email, and must only be collected if the purpose for collection is directly related to one of our functions or activities.

4.3.2 Under section 4(5) of the PPIP Act, and section 10 of the HRIP Act, any unsolicited personal information that is received from Council is not considered to be a 'collection' for the purposes of the relevant Act.

4.3.3 Council's functions and activities include:

(a) levying and collecting rates;

(b) providing services (for example, childcare, libraries and waste collection);

(c) consultation with the community, businesses and other stakeholders;

(d) assessing development and major project applications;

(e) recording, investigating and managing complaints and allegations;

(f) site inspections and audits;

(g) incident management;

(h) enforcing regulations and legislation;

(i) issuing approvals, consents, licenses and permits;

(j) providing grants;

(k) taking payments and processing reimbursements;

(l) operating surveillance devices such as Closed-Circuit Television (CCTV) cameras and other technology we use for safety and operational purposes, such as assisting with the safety of Council employees, Councillors and members of the public;

(m) preparation for closed and open Council meetings and otherwise discharging our obligations, and performing our functions and activities under the Local Government Act as a local council;

(n) dealing with legal issues and legal proceedings which Council is involved in and reporting on those issues;

(o) conducting marketing activities via our social media accounts and other means;

(p) other community engagement activities; and

(q) maintaining the non-residential register of electoral information.

4.3.4 For the types of information Council collects, see section 3 above.

4.3.5 Personal and health information may be collected from you in the following ways through:

(a) written correspondence, in person, over the phone or via email;

(b) incident reports;

(c) medical assessment reports and medical certificates;

(d) employee and Councillor reimbursement forms (including through our internal web platform);

(e) other documentation related to employment with Council;

(f) submissions;

(g) application forms;

(h) CCTV footage and other surveillance technologies (for example, at times, in-car cameras and body cameras;

(i) financial transaction records including via payment authorisation forms and requests for reimbursement from Councillors;

(j) contracts;

(k) customer enquires;

(l) use of our services and facilities (for example, if you use our childcare or pool facilities, we may collect necessary health information);

(m) online services such as the “Your Say” web form on Council’s website;

(n) contact tracing under NSW Public Health Orders; and

(o) public registers.

4.3.6 Council may collect personal information from:

(a) members of the public;

(b) businesses;

(c) NSW and Commonwealth public sector agencies;

(d) non-government organisations;

(e) employees and Councillors; and

(f) medical professionals.

4.3.7 Council will assess whether the information is needed on a case-by-case basis, in order to minimise the amount of personal and health information Council collects and manages. Council takes steps reasonable in the circumstances to ensure that, with regard to the purposes for which the information is collected, the information we collect is relevant to that purpose, is not excessive or an unreasonable intrusion on your privacy, and is accurate and up to date. Reasonable steps include making the provision of some information optional without impacting service provision, allowing people to unsubscribe or opt out of communications and reporting on information collected in a collated form to protect personal information.

4.3.8 Generally, Council will collect information from the individual directly. However, personal information may be provided by a third party. For example, a resident may provide personal information about other residents when making a complaint. Complaints often relate to parking, construction work, compliance-based issues with a property, or submissions in relation to Development Applications.

4.3.9 Generally, Council will collect health information from the individual directly. However, health information may be provided by a third party. For example, a resident may, unsolicited, provide health information about a family member or neighbour when making a submission or complaint. Where health information is collected from a third party this will generally be in consultation or cooperation with the individual, for example for the management of workers compensation claims, return to work requirements or pre-employment medicals.

4.3.10 We may also collect personal or health information from other government agencies and departments. For example, the IPC may provide us with personal or health information about you in response to an informal complaint or as part of a formal internal review. We may also collect information as a result of legal proceedings, including those conducted in the New South Wales Civil and Administrative Tribunal (**NCAT**).

### 4.4 Privacy Collection Notice (IPP 3, HPP 4)

4.4.1 When Council collects your personal or health information Council will take steps as are reasonable in the circumstances, to ensure that you are aware of the following:

(a) that Council is collecting your personal information;

(b) the purpose(s) for which your information is being collected;

(c) the intended recipients of your information;

(d) whether supplying your information is voluntary or required by law; and

(e) your right to access and correct your information.

4.4.2 To ensure that Council complies with its obligations under IPP 3, a privacy collection notice is included on Council forms, letters, documents and other records that collect personal information.

4.4.3 Please see a sample of a Privacy Collection Notice used by Council at **Attachment 2**.

4.4.4 As part of Council's commitment to continually reviewing its privacy policies, procedures and processes, Council will continue to actively consider and review its collection notices to ensure they represent privacy best practice and to ensure that individuals are clearly made aware of how Council will handle their personal and health information.

4.4.5 In some circumstances where you contact us via phone, you may be given notice verbally of the matters specified in paragraph 4.4.1, including that Council is collecting your personal information for a particular purpose.

### 4.5 Use of personal information and health information (IPPs 9, 10; HPPs 9, 10)

4.5.1 We may use personal information:

(a) for the primary purpose for which it was collected (for example, to deliver a service to you or process your application); or

(b) for a directly related secondary purpose (such as administrative activities (for example, billing or processing disbursements)); or

(c) if Council reasonably believes that the use is necessary to prevent or lessen a serious and imminent threat to life or health (for example, a member of the public, staff or Councillor suffers a medical episode at one of Council's venues we own or operate, or at an event we are promoting); or

(d) for another purpose for which the person has provided their consent.

4.5.2 For example, Council may use personal and health information for internal purposes (such as preparing documentation and reports for committees within Council), or in certain circumstances where it provides this information to its contracted services provider(s). For example, Council contracts the provision of key waste management services to a third party. To facilitate this service your personal information may be provided to that third party.

4.5.3 Council employees, contractors, service providers and Councillors should check with the Privacy Contact Officer if they are not sure if the use of information is permitted.

4.5.4 We make sure personal information is accurate before using it. For example, Council checks contact details directly with a person to make sure the information is correct and will ask people to spell their names where necessary. This is to make sure information and correspondence is sent to the right person.

4.5.5 For example, Council may use your information to improve our services by informing us of our customer needs, or to inform you about services or information available (e.g. newsletters).

4.5.6 Council's staff use the personal information collected to:

(a) deliver services;

(b) conduct research;

(c) provide advice;

(d) process payments and reimbursements;

(e) enforce Council regulations; and

(f) continually improve services offered by Council.

4.5.7 Council will also use personal information for a range of administrative, management and operational purposes which relate to our functions and activities as a local council. This includes:

(a) preparation of meeting agendas, reports and other documentation (including for committees within Council);

(b) administering billing and payments and debt recovery;

(c) planning, managing, monitoring and evaluating our services;

(d) quality improvement activities;

(e) statistical analysis and reporting;

(f) training staff, contractors and other workers;

(g) risk management and management of legal liabilities and claims (for example, liaising with insurers and legal representatives);

(h) responding to enquiries and complaints regarding our services;

(i) verifying identities where this is required (for example, to provide parking permits);

(j) obtaining advice from consultants and other professional advisers; and

(k) considering and responding to subpoenas, and other legal orders and obligations.

4.5.8 We may also use your personal information for other purposes explained at the time of collection (such as in a specific privacy collection statement or notice) or otherwise as set out in this PMP.

***Customer records***

4.5.9 For **customer records** (see section 3.2 of this PMP), as general principle we use the personal and health information we have collected only for the purpose for which it was collected. For example, if you have provided your personal information to process a development application, we will use your personal information to process your application and otherwise manage our relationship with you in relation to that development application.

4.5.10 We may also use personal and health information for directly related secondary purposes, such as auditing, reporting or program evaluation. For example, if the primary purpose of collecting a complainant's information was to investigate their customer complaint, then independent auditing of our complaint-handling practices would be an acceptable use for a directly related secondary purpose.

4.5.11 With a customer's consent, we may also use their personal information for other purposes.

***Employee and contractor records***

4.5.12 For **employee and contractor records** (see section 3.3 of this PMP), personal and health information is used by Council, including relevant division heads and reporting lines and the human resources unit, generally for workforce management.

4.5.13 This may include salary payments, wellbeing in the workplace, and performance management.

4.5.14 Staff may access certain information directly via IT systems (such as pay slips, leave balances, timesheets, and other types of personal information). You are also entitled to access your personnel file or any other related human resources or employee safety and wellbeing files that contain your personal or health information.

4.5.15 You can request access to, and amend, your personal or health information at any time by contacting the Privacy Contact Officer (see section 2.5 for contact details). This information will be updated without excessive delay.

***Councillor records***

4.5.16 For **Councillor records** (see section 3.4 of this PMP), we generally use your personal and health information for the primary purpose it was collected.

4.5.17 For example, if you are part of a committee, we would use your information to prepare the agenda, conduct relevant meetings and document the outcomes of the meeting (including your opinions and what you said at the meeting).

4.5.18 We may also use your information for a directly related secondary purpose, such as for administration purposes.

***Exemptions***

4.5.19 As specified in further detail in section 4.2 above, there are certain exemptions we may rely on in relation to use of your personal information including:

(a) if another law authorises, requires, implies, or reasonably contemplates the use (for example, laws relating to local Councils including the Local Government Act);

(b) for some law enforcement and investigative purposes (for example, to investigate suspected fraud); or

(c) for some research purposes, subject to approval by a Human Research Ethics Committee.

## 4.6 Disclosure of personal and health information (IPP 11; HPP 11)

4.6.1 Under law, Council discloses information when it provides the information to a person or body who did not previously know the information (for example, if Council publishes meeting minutes or reports on its website that contain personal information, this may be considered to be a disclosure).

4.6.2 Council will not disclose personal information without consent, unless:

(a) the disclosure is directly related to the purpose for which the information was collected, and there is no reason to believe the individual would object to the disclosure;

(b) the individual is reasonably likely to have been aware that the information of that type is usually disclosed to that other person or body (for example Councillors are aware the ways in which their personal information may be disclosed as a function of normal Council operations, such as conducting meetings);

(c) the disclosure is necessary to prevent imminent threat to the life or health of an individual; or

(d) the disclosure is permitted under the PPIP Act, or HRIP Act, or other legislation.

4.6.3 Council will generally not disclose sensitive personal or health information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities without consent, unless such disclosure is necessary to prevent or lessen an imminent threat to life or health.

4.6.4 Council will generally not disclose health information outside NSW unless such a disclosure is necessary to prevent or lessen an imminent threat to life or health, or is required under specific legislation.

4.6.5 Council does not currently have any Memorandums of Understanding or referral arrangements with other agencies. Should any such arrangements be put in place it will be done with regard to the requirements of this Privacy Management Plan.

4.6.6 Set out below are some examples of Council's typical disclosures of personal and health information, setting out to whom Council discloses the information, and some of the reasons for those disclosures:

(a) **General public** – Council publishes materials and documentation relating to certain meetings on its website (such as papers produced for and by its committees). Under law, Council is required to conduct certain meetings, and some of these meetings may be open or closed. In any case, depending on the meeting and in order to comply with our obligations under the Local Government Act, we generally publish the agenda and minutes of meetings as well as recordings and other materials in connection with open meetings on our website. These materials generally contain a range of personal information about Councillors, Council staff and the general public.

(b) **Service providers** – We may disclose personal information to a range of service providers who assist us to perform our functions and activities as a local council. These include IT service providers, marketing service providers, lawyers, accountants and other professionals. We ensure that when Council enters into contractual arrangements with such service providers, these service providers are required to comply with and understand our privacy obligations.

(c) **Other agencies and government departments** – Depending on our interaction with you, we may need to disclose your personal or health information to another agency or Government department as part of our service delivery to you.

(d) **IPC, Privacy Commissioner and NCAT**– In certain circumstances we may need to disclose your personal and/or health information to the IPC, Privacy Commissioner or NCAT (for example, in relation to privacy complaints and internal reviews (see section 6 of this PMP)). In circumstances where Council is involved in matters before NCAT, Council will have regard to NCAT's policies in regards to Council's use and disclosure of personal and health information (for example, see NCAT's policy titled "*Confidentiality, privacy and publication"*).

***Exemptions***

4.6.7 As specified in further detail in section 4.2 above, there are certain exemptions we may rely on in relation to disclosure of your personal information. A common exemption that Council will rely on to disclose personal information without consent is because we are lawfully authorised, required or otherwise permitted to disclose information under another law. For example, under the Local Government Act, Council is required to comply with certain obligations, including to conduct meetings that are open to the public and provide certain information.

## 4.7 Public registers

4.7.1 The PPIP Act also has specific requirements for personal and health information contained in public registers. A public register is a register of personal information or health information that is required by law to be made, or is made, publicly available or open to public inspection.

4.7.2 The PPIP Act prevents Council from disclosing any personal and health information contained in a public register, unless Council is satisfied that the information will be used for a purpose relating to the purpose of that register, or the Act under which that register is kept.

4.7.3 Council maintains various registers, which are maintained to fulfil our functions and activities, and as required by legislation binding on us. These registers may be updated from time to time, and may be accessed via our website, or through contacting Council (see contact details in section 2.5). These registers include the following:

***Registers available on Council's website***

4.7.4 The registers that are available on Council's website include the following:

(a) Delegations Register;

(b) Investment Registers;

(c) Registers of voting on planning matters kept in accordance with s 375A of the Local Government Act;

(d) Register of current declaration of disclosures of political donations (s 328A of the Local Government Act); and

(e) Food Premises Register.

***Registers available for inspection, free of charge and by appointment***

4.7.5 The registers that are available for inspection, free of charge and by appointment include the following:

(a) Councils Land Register (ss 53 and 54 of the Local Government Act);

(b) Register of Disclosures of Interest (s 450A of the Local Government Act);

(c) Development Consent Register (s 100 of the Environmental Planning and Assessment Act);

(d) Gifts and Benefits Register; and

(e) Register of Graffiti Removal Work.

***Suppression of personal or health information contained in a register***

4.7.6 You have the right to request that your personal or health information that is kept on a register be suppressed. Council will comply with the request if it is satisfied that your safety or wellbeing would be affected by not suppressing the information.

4.7.7 Applications to supress personal or health information from a public register should be made in writing addressed to the Privacy Contact Officer (see section 2.5 for contact details). Please include any supporting documentation (e.g., Apprehended Violence Order) in your request.

4.7.8 If you are unhappy with the determination of your request, you may seek an internal review of Council's decision (see section 6.1 - Internal review).

**4.8 Storage and security of personal and health information (IPP 5; HPP 5)**

4.8.1 Council stores personal and health information electronically and in hard copy files.

4.8.2 As part of the ongoing Recordkeeping Review and work being conducted by our Infosec Working Group, we anticipate our systems and processes involving the

storage of personal and health information will improve over time, particularly as new policies and procedures are adopted and training and education takes place to support such new policies and procedures.

4.8.3 To keep your information secure, Council aims to take the measures specified below.

***For both hard copy and electronic information***

4.8.4 Only Council employees and authorised third parties can access personal and health information.

4.8.5 Council does not collect or hold health information in a health records linkage system. Were Council to do so in the future the health records linkage system would only be used if you have provided or expressed consent for Council to do so.

4.8.6 Employees are provided with general training and ongoing fit-for-purpose training relevant to their relevant role to ensure they are complying with security measures, record keeping requirements and policies relating to privacy.

4.8.7 Personal and health information will be kept no longer than necessary, and disposed of appropriately in accordance with Council's Retention and Disposal Authorities and applicable laws.

4.8.8 We train and educate our staff and Councillors on the consequences of accessing or disclosing information for an unlawful purpose (i.e., leaking information).

4.8.9 Council's staff and Councillors must use Council-issued systems and processes for conducting Council business, unless expressly authorised otherwise. Council may refuse requests from Councillors or staff to use an unsecure method (for example requests to email documents to a Councillor's personal email accounts, or to print documents without Council-issued watermarks which identify who has printed the document).

***Hard copy***

4.8.10 Hard copy files are mainly located in Council's Main Office at 200 Miller Street North Sydney and at our offsite depot located at 187 Ernest Street North Sydney (**Depot**).

4.8.11 Council's offices are adjacent to our customer service area which is open to the public. The offices, however, require key card access, and visitors cannot access them without permission. The entire building is locked outside of business hours.

4.8.12 Hard copy files located at the Depot are only accessible by a limited number of Council employees who have authority to access them. Other staff members must make a written request to have hard copy files retrieved from the Depot, and those documents are monitored while in use, then returned to the Depot once no longer required.

4.8.13 Physical access to the Depot is recorded via swipe card access and logbook entries.

4.8.14 Hard copy files that must be kept are archived at the Deport in compliance with the *State Records Act 1998* (NSW) and other applicable laws.

4.8.15 When hard copies of personal and health information are in transit between the Deport and Council's Main Office, they are kept in a secure vehicle or case.

4.8.16 Only authorised Council employees and authorised third parties can access personal and health information.

4.8.17 Documents containing personal or health information are stored in a secure area of Council's Main Office or at the Depot when not in use.

4.8.18 Hard copies of personal and health information are destroyed as soon as is practicable after the information has been digitised or is no longer needed.

4.8.19 Staff are trained to implement a 'clean desk' approach to minimise unsecure hard copy papers and records being stored on desks and other areas when not in use.

4.8.20 We minimise the time hard copies containing personal information are stored by destroying these copies once no longer required (for example at our Customer Service desk, if credit card information is stored on paper forms, this is stored under lock and key and promptly and securely destroyed once digitised or otherwise processed).

4.8.21 Staff are trained to ensure secure storage facilities are properly locked.

4.8.22 Secure storage areas are monitored to determine who has accessed secure store areas and when access took place.

4.8.23 Council also actively considers how it can continually improve its processes – for example, Council recently introduced a secure electronic form to process Councillors' requests for reimbursements to reduce the handling of physical receipts and other hard copy documents.

4.8.24 Secure bins are available onsite to dispose of documents containing personal or health information that are no longer required.

***For electronic copies***

4.8.25 There are a range of systems in place across Council that are used to create, house, and maintain records (inclusive of personal and health information). Some of the main systems Council use include:

(a) **ECM – TechnologyOne** - ECM – Recordkeeping system supporting capture and distribution of wide range of Council records.

(b) **Authority – Civica –** Wide range of functions including financial management, procurement and contracts, property and rating, applications, HR hierarchy manager, payroll, asset management, receipting, name and address register, general ledger, basic CRM.

(c) **Microsoft 365 –** Communication and collaboration platform spanning a range of solutions. Outlook a key tool supporting email communications.

4.8.26 As part of the roll-out of the Recordkeeping Review, Council is in the process of implementing a range of recommendations, including in relation to ECM.

4.8.27 At the time of publication of this PMP, key security measures for electronic storage of personal and health information include the following:

(a) electronic information can only be accessed by Council's employees and authorised third parties;

(b) electronic information will be stored on secure information systems;

(c) Council is in the process of implementing multi-factor authentication (**MFA**) to access devices, systems and accounts;

(d) employees and Councillors are required to have unique user accounts, and use complex passwords that are changed frequently. Our staff do not give out passwords to anyone or let anyone else use their computer login;

(e) access to shared email inboxes is reviewed annually, and when there is a change of position or new starter;

(f) employee and contractor access to both Council office and IT systems is removed promptly if they cease employment or engagement with Council;

(g) employees and Councillors must ensure Council business is not conducted on personal email, social media accounts and messaging apps;

(h) employees and councillors must use Council-controlled systems to conduct Council business;

(i) systems are monitored for unauthorised access, viruses, and malicious code and other types of potential or actual data breaches or incidents;

(j) ongoing training and education of staff about potential security risks (such as phishing scams);

(k) ongoing training as part of the Recordkeeping Review, including the best practice use of Council's core systems such as ECM;

(l) systems retain a record of users who have accessed files, records and Council's computer systems; and

(m) Council's IT department conducts security penetration testing on digital systems and conducts periodic review of security controls.

**4.9 Accessing or amending your personal and health information (IPPs 6, 7, 8; HPPs 6, 7, 8)**

4.9.1 You have the right to ascertain whether Council holds your personal and health information, the nature of that information, and the main purpose for which it was collected.

4.9.2 You have a right to access your personal and health information that Council holds. You can also request that the information be amended, for example to update your contact details.

4.9.3 If you wish to understand, access or amend your personal or health information held by Council, please contact Council's Privacy Contact Officer in writing (see section 2.5 for contact details). If you are requesting amendments, please include the details of those amendments.

4.9.4 There are no fees for making the request to access or amend your personal and health information. Council will endeavour to respond to your request within 7 business days.

4.9.5 Upon receiving your request for amendments, Council must make appropriate amendment(s) (by way of corrections, deletions or additions) to ensure that the personal information is:

(a) accurate; and

(b) relevant, up to date, complete, and not misleading having regard to the purpose for which the information was collected.

4.9.6 If Council decides to not amend the information, your request for amendment will be attached to your existing information (so that it can be read with your existing information).

### 4.10 Accessing or amending other people's information

4.10.1 Generally, you can only access or amend your own personal or health information. However, section 26 of the PPIP Act does allow you to give consent to Council to disclose your personal information to someone else.

4.10.2 Sections 7 and 8 of the HRIP Act allows an 'authorised representative' to act on your behalf.

---

## 5. Data breaches

### 5.1 What is a data breach?

5.1.1 A data breach occurs when there is a failure that caused or has the potential to cause unauthorised access to Council's physical or electronic information. Common examples of a data breach can include malware, hacking or data theft, but breaches can also be caused by human or technical errors. Other examples of data breaches include:

(a) accidental loss or theft of information or equipment;

(b) sending an email to the wrong email list;

(c) a staff member or Councillor intentionally leaking documents containing personal information;

(d) leaving unsecured documents or tapes unattended in a public place;

(e) unauthorised use, access to or modification of data or information systems to gain unauthorised access or make unauthorised changes; or

(f) disruption to or denial of IT services.

### 5.2 Responding to a data breach

5.2.1 Unlike the privacy regime under the Commonwealth Privacy Act (which only applies to Council in respect of Tax File Numbers), at the time of publication of this PMP, there is no mandatory data breach notification regime in NSW.

5.2.2 Council acknowledges that a mandatory data breach notifications scheme in NSW is likely in the near future with the relevant laws currently in the consultation phase.

5.2.3 Council instead aims to respond to data breaches in accordance with our legal obligations and guidance from the IPC.

5.2.4 Council, upon becoming aware of a data breach, will:

(a) act to contain the breach; and

(b) conduct an assessment, to determine whether the breach is likely to cause serious harm and what response should be taken.

5.2.5 Each data breach is different, but Council will manage a data breach by following the key steps recommended in IPC guidance:

(a) **Contain** – Council will take all necessary steps possible should to contain the breach and minimise any resulting damage. This includes, for example, recovering the personal information, shutting down the system that has been breached, suspending the activity that led to the breach, or revoking or changing access codes or passwords.

(b) **Evaluate** – Council will consider the type of data breach, who is affected, what caused the breach, and what are the specific risks that could follow., to determine its next steps This will include a broad scope assessment of the breach and may include looking at external systems, website and storage drives if they were a factor in the breach. For example, a breach of contact information alone is unlikely to cause serious harm, whereas access by a malicious party to a combination of data types will typically create a greater potential for harm.

(c) **Notify** – While not compulsory in NSW, notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations. In general, if a data breach creates a serious risk of harm to an individual/organisation, Council will consider voluntary notification to those affected.

5.2.6 Where the breach involves Tax File Numbers, Council will consider its obligations under the Commonwealth Privacy Act, which regulates Tax File Numbers and determine if mandatory notification under that regime is required.

5.2.7 When responding to data breaches, Council will also endeavour to follow the policies and procedures being developed by the Infosec Working Group (which is using well recognised standards and policies as part of this process), including the draft Incident Management Policy (or final Incident Management Policy once adopted). These policies include:

(a) ISO. 2015. “ISO/IEC 27000:2016(E) Information technology - Security techniques - Information security management systems - Overview and vocabulary.” Geneva: ISO.

(b) 2016. “ISO/IEC 27035-1:2016(E) Information technology - Security techniques - Information security incident management – Part 1: Principles of incident management.” Geneva: ISO.

(c) 2016. “ISO/IEC 27035-2:2016(E) Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response.” Geneva: ISO.

(d) Standards Australia. 2015. “AS ISO/IEC 27001:2015 Information technology - Security techniques - Information security management systems - Requirements.” Sydney: SAI Global Ltd.

## 6. Your rights: complaints and review

### 6.1 Internal review

6.1.1 You have a right to request an internal review under Part 5 of the PPIP Act if you believe Council has breached the PPIP Act or the HRIP Act.

6.1.2 An internal review is an investigation that Council conducts into a complaint. During the review Council will:

(a) assess whether or not it has complied with its privacy obligations; and

(b) inform the complainant of its findings and any actions Council will take as a result.

### 6.2 Applications for internal review

6.2.1 You can request an internal review by contacting Council's Privacy Contact Officer.

**IMPORTANT NOTE**
Applications for internal review **must be in writing**. Therefore these applications must be provided to the Privacy Contact Officer by post, email or delivery to Council's offices, and not by phone or verbally to our customer service team.

6.2.2 All written complaints we receive about Council's handling of personal or health information will be considered an application for an internal review, even if you do not use the words 'internal review' or specifically refer to privacy legislation. However, the complaint must, on its face, reasonably convey to Council that an application for internal review is sought.

6.2.3 Under the PPIP Act, applications for an internal review must:

(a) be in writing;

(b) be addressed to Council;

(c) include your postal address or email address so that we can contact you with our response; and

(d) be made within 6 months from first becoming aware of the conduct that is the subject of the application. However, depending on circumstances, Council may also consider a late application for internal review.

6.2.4 We recommend that you use the IPC's *Privacy Complaint: Internal Review Application Form* when submitting a written request for a review with Council. This form is attached to this PMP at **Attachment 3**. It can also be found on both our website and the IPC's website. Although we encourage you to use this form, it is not compulsory.

### 6.3 What you can expect from us

6.3.1 Council will aim to:

(a) acknowledge receipt of the application within **5 business days**; and

(b) complete the internal review within **60 calendar days**.

6.3.2 Once Council has completed the review, we will respond to you in writing within **14 calendar days** of deciding the outcome of the internal review.

6.3.3 If you disagree with the outcome, or you do not receive a response within **60 calendar days** of making your application for internal review, you have the right to seek internal review.

### 6.4 Who conducts the internal review?

6.4.1 In most circumstances the Privacy Contact Officer will conduct the internal review. However, if the internal review concerns the conduct of the Privacy Contact Officer, another member of Council staff will be appointed to conduct the internal review.

6.4.2 If the application for internal review is made by a person who is either:

(a) a Councillor; or

(b) an employee of Council,

then the Privacy Contact Officer may engage an independent external reviewer to provide advice on the internal review prior to finalising the internal review.

It is noted that the Information and Privacy Commission has advised that unless there are exception circumstances the Privacy Commissioner would generally not exercise the discretion under section 54(3) of the PIPP Act to undertake an internal review.

6.4.3 Where it is not practicable for an employee of Council, whether the Privacy Contact Officer or other, to conduct the internal review the internal review can be referred to an independent external reviewer. (CRE v Blacktown City Council [2017] NSWCATAD 285)

### 6.5 How is internal review conducted?

6.5.1 The Privacy Contact Officer or the person appointed to conduct the review will refer to the IPC guidance materials while conducting the review, including the IPC's Checklist: Internal Review.

6.5.2 Under s 54 of the PPIP Act, Council is required to inform the Privacy Commissioner of an application for internal review and provide updates on the internal review's progress.

6.5.3 We have briefly summarised the internal review process below:

(a) Upon receiving the request, the Privacy Contact Officer will acknowledge receipt of the application and notify the Privacy Commissioner of the application.

(b) The Privacy Contact Officer will then conduct a preliminary assessment of the request. This assessment determines:

(i) whether the complaint concerns personal or health information and whether the PPIP or HRIP Act will apply;

(ii) when the alleged conduct occurred;

(iii) whether the request was lodged within 6 months of the conduct; and

(iv) whether it is appropriate for the Privacy Contact Officer to conduct the review, or whether the application needs to be referred to another Council employee or the Privacy Commissioner.

(c) If the application needs to be referred to another Council employee or to the Privacy Commissioner, this will be done promptly after the preliminary assessment.

(d) Once the preliminary assessment has been completed, the Privacy Contact Officer will write to the Complainant informing them of:

(i) Council's understanding of the conduct complained;

(ii) the Privacy Principle(s) at issue;

(iii) whether Council or the Privacy Commissioner is conducting an internal review under either the PPIP Act or HRIP Act, as appropriate;

(iv) the name, title and contact details of the reviewing officer or the Privacy Commissioner;

(v) their rights, if the review is not completed within 60 days, to seek external review by NCAT; and

(vi) the fact that their application will be provided to the Privacy Commissioner.

(e) At this stage, if Council is conducting the review, the Privacy Contact Officer will also endeavour to provide an update to the Privacy Commissioner on the preliminary assessment and the next steps Council will take.

(f) The Privacy Contact Officer or the person conducting the review will then undertake the internal review in accordance with the IPC's checklist. The internal review will determine the following questions:

(i) whether the alleged conduct occurred;

(ii) if so, whether the conduct complied with the relevant Privacy Principles; and

(iii) if the conduct did not comply, whether the non-compliance was authorised by:

(A) an exemption under the relevant Act;

(B) a privacy code of practice; or

(C) a s 41 PPIP Act Direction from the Privacy Commissioner.

(g) Four weeks after notifying the Privacy Commissioner, the Privacy Contact Officer or the person conducting the review will send a progress report to both the Privacy Commissioner and the complainant outlining the progress of the review, advising of any delays, and reminding the complainant of their rights to seek external review by NCAT if the review is not completed within 60 days.

6.5.4 Once the internal review has been completed, Council may decide to take no further action, or it may decide to take one or more of the following actions:

(a) make a formal apology;

(b) take remedial action;

(c) provide undertakings that the conduct will not occur again; or

(d) implement administrative measures to reduce the likelihood of the conduct occurring again.

6.5.5 The Privacy Contact Officer or the person conducting the review may send preliminary findings to the Privacy Commissioner.

6.5.6 After conducting the review, the Privacy Contact Officer or the person conducting the review will contact you in writing within **14 calendar days** of completing the internal review informing you of:

(a) their findings;

(b) any actions that will be taken as a result of the findings; and

(c) the rights you have to have the findings and any proposed actions reviewed by the NSW Civil and Administrative Tribunal.

6.5.7 A final copy of the review will also be sent to the Privacy Commissioner.

6.5.8 If you are not satisfied with Council's findings, you have a right to make an application to the NCAT for an external review of Council's findings (see further below in section 6.7).

### 6.6 Role of the NSW Privacy Commissioner

6.6.1 Council must notify the Privacy Commissioner of any internal reviews being conducted and inform the Privacy Commissioner of Council's findings and any proposed actions. We will keep the Privacy Commissioner informed of the progress of the review in accordance with the summary above in section 6.5.

6.6.2 The Privacy Commissioner may make submissions to Council in relation to the subject matter of the internal review.

6.6.3 If the Privacy Commissioner undertakes an internal review at Council's request, Council will accept and implement the Privacy Commissioner's recommended course of action (which is provided as part of their review).

### 6.7 External review by the NSW Civil & Administrative Tribunal (NCAT)

6.7.1 You are able to request for the internal review outcome to be reviewed by NCAT if you are unhappy with the findings, or if you do not receive an outcome within 60 days of your application.

6.7.2 If you would like the internal review outcome reviewed, you will need to apply directly to NCAT for an external review within **28 days** from the date of the internal review decision.

6.7.3 To apply for an external review or to obtain more information, please contact NCAT:

**Website:** https://www.ncat.nsw.gov.au/

**Phone:** 1300 006 228

**Visit:** Level 10 John Maddison Tower, 86-90 Goulburn Street, Sydney NSW.

### 6.8 Other ways to resolve privacy concerns

6.8.1 Council wishes to engage with members of the public to discuss any concerns you might have about privacy. We encourage you to try and resolve any privacy issues you have with us informally before lodging an internal review.

6.8.2 You can raise your concerns and seek an informal resolution by contacting the Privacy Contact Officer, or using the online feedback form available on our website.

6.8.3 Please keep in mind that you have **six months** from when you first became aware of the potential breach to seek an internal review of the incident, and that this six month period accrues even if you are working with Council to informally resolve the issue. Please consider this time limit when deciding whether to make a request for internal review or continue working with Council to find an informal resolution.

## 7. Contacts

| Contact | Contact details |
|---|---|
| **North Sydney Council's Privacy Contact Officer** | **Phone:** 02 9936 8100<br>**Facsimile:** 02 9936 8177<br>**Email:** council@northsydney.nsw.gov.au<br>**Address:** North Sydney Council, PO Box 12, North Sydney, NSW, 2059 |
| **The Information and Privacy Commission NSW** | **Phone:** 1800 472 697<br>**Email:** ipcinfo@ipc.nsw.gov.au<br>**Website:** https://www.ipc.nsw.gov.au/<br>**Office:** Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 |
| **NSW Civil and Administrative Tribunal (NCAT)** | **Phone:** 1300 006 228<br>**Email:** aeod@ncat.nsw.gov.au<br>**Address:** Level 10 John Maddison Tower, 86-90 Goulburn Street, Sydney NSW.<br>**Website** https://www.ncat.nsw.gov.au/ |

**IMPORTANT NOTE**
Applications for Internal Review **must be in writing**. Therefore these applications must be provided to the Privacy Contact Officer by post, email or delivery to Council's offices. Please see section 8.2 for further information.

# Attachment 1 Definitions

| Definitions | |
|---|---|
| **Council** | means North Sydney Council. |
| **Councillor** | means Council's elected representatives. |
| **health information** | means information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or health services or a health service provided or to be provided to a person. See section 6 of HRIP Act. |
| **Health Privacy Principles (HPPs)** | means the 15 HPPs contained in Schedule 1 of the HRIP Act, which NSW public sector agencies and private sector organisations must comply with when they collect, hold, use or disclose a person's health information. |
| **Information Privacy Principles (IPPs)** | means the 12 IPPs contained in Part 2, Division 1 of the PPIP Act, which NSW public sector agencies, statutory bodies, universities and local councils must comply with when they collect, hold, use or disclose personal information. |
| **IPC** | means the Information and Privacy Commission NSW, an independent statutory authority that administers legislation dealing with privacy and access to government held information in New South Wales. |
| **personal information** | means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. See section 4 of the PPIP Act. |
| **Privacy Principles** | means the IPPs and the HPPs. |
| **Privacy Commissioner** | means the individual appointed as the NSW Privacy Commissioner and responsible for administering the PPIP Act and the HRIP Act. |
| **PMP** | means this Privacy Management Plan. |
| **Recordkeeping Review** | has the meaning given to that term in section 2.2.4 of this PMP. |
| **sensitive information** | means information about an individual's ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership. |

# Attachment 2 Sample collection notice

*As part of Council's commitment to continually reviewing its privacy policies, procedures and processes, Council will continue to actively consider and review its collection notices (including the example provided below), to ensure they represent privacy best practice and to ensure that individuals are clearly made aware of how Council will handle their personal and health information.*

## North Sydney Council's Privacy Statement

PRIVACY STATEMENT

North Sydney Council is collecting your personal information for the purposes of processing an application or submission. The supply of personal information is entirely voluntary. If you elect not to provide or do not wish to provide your personal information, Council may not be able to process your application or act on or acknowledge your submission. North Sydney Council shall be regarded as the agency that holds your personal information and access to your personal information by interested parties, may be released in line with Council policies. North Sydney Council may publish any personal information included in a submission on a proposal or proposed development. You have a right to access your personal information held by Council. You also have a right to have your personal information corrected or amended by Council. Applications by members of the public to view Council's records which are not in the public arena are subject to the provisions of *Privacy and Personal Information Protection Act 1998*, *Government Information (Public Access) Act 2009* and North Sydney Council's Privacy Management Plan.

I have read and understand the Privacy Statement Signed:
.....
Date:.....

# Attachment 3 IPC Internal review form

information and privacy commission new south wales

**Application Form** **Updated September 2019**

## Privacy Complaint: Internal Review Application Form

This is an application[1] for review of conduct of an agency under: (please select one)

- ☐ s53 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- ☐ s21 of the *Health Records and Information Privacy Act 2002* (HRIP Act)

Your completed form must be sent to the Agency listed in Question 1 below.

| | |
|---|---|
| 1 | Name and address of the agency[2] you are complaining about: |
| 2 | Your full name: |
| 3 | Your postal address:<br>Telephone number:<br>Email address: |
| 4 | If the complaint is on behalf of someone else, please provide their details:<br><br>What is your relationship to this person (eg. parent)?<br><br>Please include details of your authority to act or make the complaint on behalf of the person you have named above.<br><br>Is the person capable of making the complaint by himself or herself?<br>☐ yes<br>☐ no<br>☐ unsure |
| 5 | What is the specific conduct[3] you are complaining about? Describe what you believe the Agency did. *(see footnote for explanation of "conduct")* |
| 6 | Please tick which of the following describes your complaint: *(you may tick more than one option)*<br>☐ collection of my personal or health information<br>☐ security or storage of my personal or health information<br>☐ refusal to let me access or find out about my own personal or health information<br>☐ accuracy of my personal or health information<br>☐ use of my personal or health information<br>☐ disclosure of my personal or health information<br>☐ other<br>☐ unsure |

| | |
|---|---|
| 7 | When did the conduct occur (date)? *(please be as specific as you can)* |
| 8 | When did you first become aware of this conduct (date)? (*please be as specific as you can about how and when you first became aware of the conduct. Please include any action that you took at the time)* |
| 9 | You need to lodge this application within six months of the date at Q.8.<br>If more than six months has passed, you will need to ask the agency for special permission to lodge a late application. Please explain why you have taken more than six months to make your complaint *(for example: I had other urgent priorities – list them, or while the conduct occurred more than six months ago, I only recently became aware of my privacy rights, etc)*: |
| 10 | What effect did the conduct have on you? |
| 11 | What effect might the conduct have on you in the future? |
| 12 | What would you like to see the agency do about the conduct? *(for example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)* |

I understand that this form will be used by the agency to process my request for an internal review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54(1) of the *Privacy and Personal Information Protection Act*; or section 21 of the *Health Records and Information Privacy Act*; and that the Privacy Commissioner will be kept advised of the progress of the internal review.

Your signature: _____

Date:

SEND THIS FORM TO THE AGENCY YOU HAVE NAMED AT Q.1

**Keep a copy for your records.**

For more information on the PPIP Act or the HRIP Act visit our website: www.ipc.nsw.gov.au
**Freecall:** 1800 472 679
**Email:** ipcinfo@ipc.nsw.gov.au
**Website:** www.ipc.nsw.gov.au

---

1 It is not a requirement under the PPIP Act or the HRIP Act that you complete an application form. This form is designed for your convenience only. However, you must make a written request in some form to the agency for the matter to be a valid internal review.

2 The PPIP Act regulates NSW state government departments, area health services, most other state government bodies, and NSW local councils. Each of these is defined as a "public sector agency". The HRIP Act regulates private and public sector agencies and private sector persons.

3 "Conduct" can include an action, a decision, or even inaction by the agency. For example the "conduct" in your case might be a *decision* to refuse you access to your personal information, or the *action* of disclosing your personal information to another person, or the *inaction* of a failure to protect your personal information from being inappropriately accessed by someone else

# Attachment 4 Managing personal information and health information under legislation

This **Attachment 4** contains a general summary of key pieces of legislation that govern Council's management of personal information and health information.

## 1. *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act)

The PPIP Act outlines how Council must manage personal information. The PPIP Act contains 12 Information Protection Principles (**IPPs**) which Council must comply with. An overview of the IPPs is set out below (please note this is a summary only – see the PPIP Act for full text of the IPPs).

### 1.1 Collection

1.1.1 Council must only collect personal information for a lawful purpose that is directly related to Council's functions and activities, and the collection of the information is reasonably necessary for that purpose (**IPP 1**).

1.1.2 Council must collect personal information directly from the individual. Council must not collect personal information from third parties unless the individual has authorised collection from someone else or, in the case of information relating to a person under the age of 16 years, the information has been provided by a parent or guardian (**IPP 2**).

1.1.3 Council must inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. Council must tell people how they can access and amend their personal information and any possible implications if they decide not to give their personal information to us (**IPP 3**).

1.1.4 Council must ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the individual's personal affairs (**IPP 4**).

### 1.2 Retention and security

1.2.1 Council must store personal information securely, keep it no longer than necessary and dispose of it securely and in accordance with Council's obligations under the *State Records Act 1998* (NSW) and any other requirements for the retention and disposal of personal information. Council must also ensure that personal information is protected against loss, unauthorised access, use, modification or disclosure, ad against all other misuse (**IPP 5**).

### 1.3 Access and accuracy

1.3.1 Council must take such steps as are, in the circumstances, reasonable to be transparent about the personal information it holds, the purpose for which the information is used and the right for individuals to access their personal information (**IPP 6**).

1.3.2 Council must provide individuals with access their own personal information without unreasonable delay or expense (**IPP 7**).

1.3.3 Council must, at the request of individuals, update, correct or amend their personal information to ensure the information is accurate, relevant, up to date, complete, and not misleading, where appropriate (**IPP 8**).

1.3.4 Council must take such steps as are reasonable in the circumstances to ensure that personal information is relevant, accurate, complete and not misleading before using it (**IPP 9**).

**1.4 Use**

(**IPP 10**)

1.4.1 Council must only use personal information:

(a) for the purpose for which it was collected for ("the primary purpose");

(b) for a purpose other than the primary purpose ("the secondary purpose"), so long as that purpose is directly related to the primary purpose;

(c) if it believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious or imminent threat to the life or health of the individual to whom the information relates or of another person;

(d) in accordance with the PPIP Act, the HRIP Act, and as specified below in section 1.7 (Exemptions to the IPPs) and section 2 (Privacy Code of Practice for Local Government) of this **Attachment 4**; or

(e) for any other purpose only with the individual's consent.

**1.5 Disclosure**

(**IPP 11**)

1.5.1 Council must only disclose personal information :

(a) for a purpose directly related to the primary purpose, and the Council has no reason to believe the individual would object to the disclosure;

(b) if it believes on reasonable grounds that the disclosure 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; or

(c) in accordance with the PPIP Act, the HRIP Act, and as specified below in section 1.7 (Exemptions to the IPPs) and section 2 (Privacy Code of Practice for Local Government) of this **Attachment 4**.

1.5.2 Council must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

**1.6 Offences under the PPIP Act**

1.6.1 Sections 66-68 of the PPIP Act set out offences under the PPIP Act, , including the penalties (including imprisonment for up to two years', an $11,000 fine, or both) that attach to those offences. It is an offence for Council (including its employees, Councillors, and contractors) to:

(a) intentionally disclose or use personal information (otherwise than in connection with the lawful exercise of official functions);

(b) offer to supply personal information that has been disclosed unlawfully; or

(c) hinder the Privacy Commissioner or their employees from doing their job.

### 1.7 Exemptions to the IPPs

1.7.1 Part 2, Division 3 of the PPIP Act contains exemptions that may permit Council to not comply with the IPPs in certain circumstances. These include the following:

(a) Council is not required to comply with IPPs 2-3, 6-8, or 10-12 if Council is lawfully authorised or required not to do so; and

(b) Council is not required to comply with IPP 2 if the information concerned is collected in relation to court or tribunal proceedings.

1.7.2 For example, s 23(2) of the PPIP Act provides that Council is not required to comply with collection requirements if the information concerned is collected for law enforcement purposes such as the issue of a penalty infringement notice.

---

## 2. Privacy Code of Practice for Local Government

### 2.1 Privacy Code of Practice for Local Government

2.1.1 Council must comply with the Privacy Code of Practice for Local Government as prepared by the Office of the Privacy Commissioner and revised on 20 December 2019.

2.1.2 Under the Privacy Code of Practice for Local Government, where it is reasonably necessary, Council may indirectly collect and use personal information to confer an award, prize, or similar form of personal recognition on the person about whom the information relates.

2.1.3 The Privacy Code of Practice for Local Government also permits Council to use personal information for a purpose other than the purpose for which it was collected, where:

(a) the use is in pursuance of Council's lawful and proper functions; and

(b) Council is satisfied that the personal information is reasonably necessary for the exercise of those functions.

2.1.4 For example, the Rates Record that Council holds under s 602 of the Local Government Act may be used to:

(a) notify neighbours of a proposed development;

(b) evaluate a road opening; or

(c) evaluate a tree preservation order.

2.1.5 In addition, Council may use personal information for other specific purposes where Council is satisfied that the information is reasonably necessary for another function, such as:

(a) understanding community and customer needs to improve our services;

(b) letting customers know about services or other information available (e.g. newsletters); or

(c) sharing personal information within other divisions of Council and authorised outsourced service providers to expedite services to customers.

---

## 3. *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act)

The HRIP Act governs how Council must manage health information.

The HRIP Act contains 15 Health Privacy Principles (**HPPs**) that Council must comply with. An overview of the HPPs (as they apply to Council) is set out below (please note this is a summary only – see the HRIP Act for full text of the HPPs).

### 3.1 Collection

3.1.1 Council must only collect health information for a lawful purpose that is directly related to Council's functions and activities, and the collection of the information is reasonably necessary for that purpose (**HPP 1**).

3.1.2 Council must take reasonable steps to ensure that health information it collects is relevant to the purpose for collection (the "primary purpose"), is accurate, is not excessive, is up to date and complete, and does not unreasonably intrude into people's personal affairs (**HPP 2**).

3.1.3 Council must only collect information directly from the person concerned (unless it is unreasonable or impracticable to do so) (**HPP 3**).

3.1.4 Council must inform people why their health information is being collected, what it will be used for, to whom it will be disclosed, how it can be accessed and amended, and any possible implications of not providing health information (**HPP 4**).

### 3.2 Retention and security

3.3 Council must store health information securely, keep it no longer than necessary and destroy it appropriately. Council must also ensure that health information is protected against loss, unauthorised access, use, modification or disclosure, ad against all other misuse (HPP 5).

### 3.4 Access and accuracy

3.4.1 Council must take such steps as are, in the circumstances, reasonable to be transparent about the health information it holds, the purpose for which the information is used, and the right for individuals to access and amend their health information (**HPP 6**).

3.4.2 Council must provide individuals with access their own health information without unreasonable delay or expense (**HPP 7**).

3.4.3 Council must, at the request of individuals, update, correct or amend their health information to ensure the information is accurate, relevant, up to date, complete, and not misleading, where appropriate (H**PP 8**).

3.4.4 Council must take such steps as are reasonable in the circumstances to ensure that health information is relevant, accurate, complete and not misleading before using it (**HPP 9**).

### 3.5 Use and disclosure

(**HPPs 10 and 11**)

3.5.1 Council must only use and disclose health information for a purpose other than the primary purpose for which it was collected (the "secondary purpose") if the individual has consented to the use for the secondary purpose, or another relevant exception applies, such as:

(a) the secondary purpose is directly related to the primary purpose and the individual would reasonably expect Council to use the information for the secondary purpose; and

(b) the use of the information for the secondary purpose is reasonably believed by Council to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or to public health and safety.

### 3.6 Identifiers and anonymity

3.6.1 Council may only assign unique identifiers for health information if it reasonably necessary to enable Council to carry out any of its functions efficiently (**HPP 12**).

3.6.2 Council must provide individuals with the opportunity to remain anonymous, where it is lawful and practicable (**HPP 13**).

### 3.7 Offences

3.7.1 Sections 68-70 of the HRIP Act set out offences under the HRIP Act, including the penalties (including imprisonment for up to two years', an $11,000 fine, or both) that attach to those offences. It is an offence for Council (including its employees, Councillors, and contractors) to:

(a) intentionally disclose or use health information (otherwise than in connection with the lawful exercise of official functions); or

(b) offer to supply health information that has been disclosed unlawfully.

### 3.8 Exemptions to the HPPs

3.8.1 Exemptions are located mainly in Schedule 1 to the HRIP Act, and may permit Council not to comply with HPPs in certain situations. For example, Council is not required to comply with HPPs 4-8, and 10 if lawfully authorised or required not to do so.

### 3.9 Health Records and Information Privacy Code of Practice 2005

3.9.1 The Health Records and Information Privacy Code of Practice 2005 applies to Council. It permits, in certain limited circumstances, the collection, use and disclosure of health information between human services agencies without the consent of the person to whom the health information relates. A human services agency is a public sector agency that provides welfare services, health services, mental health services, disability services, drug and alcohol treatment services, housing and support services and/or education services.

## 4. Other relevant legislation

| Legislation | Description |
|---|---|
| ***Government Information (Public Access) Act 2009*** **(GIPA Act) and** ***Government Information (Public Access) Regulation 2009*** | Under this Act and Regulation, members of the public can apply to Council for access to information held by Council. The information may include personal or health information.<br>**Council employees – name and position title:** Schedule 4 of the GIPA Act also provides that information about a Council employee, including their name and non-personal contact details (such as position title and their public functions at Council) is not personal information for the purposes of the GIPA Act. |
| ***Local Government Act 1993*** **(Local Government Act)** | Council's primary responsibilities are mainly under this Act, which sets out Council's functions and activities including obligations in respect of the administration of Council. |
| ***Independent Commission Against Corruption Act 1988*** | Under this Act, Council must provide information to the Independent Commission Against Corruption about allegations of fraud and corruption that may contain personal and/or health information. |
| ***Public Interest Disclosure Act 1994*** **(PID Act)** | Under the PID Act, any public official can make a public interest disclosure to Council. The PID Act requires that information that might identify or tend to identify a person who has made a public interest disclosure should be protected. |
| ***State Records Act 1998*** **and** ***State Records Regulation 2015*** | This Act and Regulation authorise the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately. |
| **Referrals to external agencies under other relevant legislation** | Under the *Ombudsman Act 1974* (NSW), the *Independent Commission Against Corruption Act 1998* (NSW), and the *Crimes Act 1900* (NSW), Council can provide information, including personal and health information, to the:<br>▪ NSW Ombudsman;<br>▪ Independent Commission Against Corruption; and<br>▪ NSW Police. |