PRIVACY MANAGEMENT PLAN

Public Document

Version: 8 / ECM: Fixed Reference No.: 2988305

Adopted by: Council on 25 August 2000

Reviewed: 7 May 2024

Ownership: Governance

TABLE OF CONTENTS

Purpose

To outline Mosman Council's policies and practices in ensuring compliance with the requirements of the *Privacy and Personal Information Protection Act 1998* (PPIPA) and the *Health Records and Information Privacy Act 2002 (HRIPA)*.

Council collects and holds personal and health information for the purposes of facilitating its business. It is important that the use of this information is confined to the purposes for which it is acquired. Council is committed to protecting the privacy of our customers, officials, employees, volunteers and contractors.

The PPIPA provides for the protection of personal information and for the protection of the privacy of individuals. The PPIPA requires all public sector agencies to prepare, implement and review their Privacy Management Plan (Plan). This Plan outlines how Council complies with the legislative requirements of the PPIPA, HRIPA, the Privacy Code of Practice for Local Government (Code) and other legislation including the *Privacy Act 1988 (Cth)*.

This Plan also provides information about:

- who to contact if you have questions about the information collected and held by Council
- how to access and amend your information
- what to do if you believe that Council has breached the PPIP or HRIP Acts
- Council responsibilities under the Mandatory Notification of Data Breach (MNDB) Scheme to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm
- Council's privacy risk management governance framework

Objectives

This Plan has been prepared with regard to section 33 of the PPIPA and the Code to show how Council deals with personal information and health information it collects to ensure that it complies with the PPIPA and the HRIPA. It details how Council manages the personal and health information it collects, stores, accesses, uses and discloses in the course of its business activities.

Scope

To inform:

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

Whilst this document is called a Privacy Management Plan in accordance with the legislative requirements, for the purpose of Council it is considered a Policy.

1.0 Introduction

The PPIPA provides for the protection of personal information and for the protection of the privacy of individuals.

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

- The devising of policies and practices to ensure compliance by the Council with the requirements of the PPIPA and the HRIPA.

- The dissemination of those policies and practices to persons within the Council.

- The procedures that the Council proposes for internal review of privacy complaints.

- Such other matters as are considered relevant by the Council in relation to privacy and the protection of personal information held by it.

This Plan has been prepared for the purpose of section 33 of the PPIPA. PPIPA provides for the protection of personal information by means of 12 Information Protection Principles. Those principles are listed below:

Principle 1 - Collection of personal information for lawful purposes
Principle 2 - Collection of personal information directly from individual
Principle 3 - Requirements when collecting personal information
Principle 4 - Other requirements relating to collection of personal information
Principle 5 - Retention and security of personal information
Principle 6 - Information about personal information held by agencies
Principle 7 - Access to personal information held by agencies
Principle 8 - Alteration of personal information
Principle 9 - Agency must check accuracy of personal information before use
Principle 10 - Limits on use of personal information
Principle 11 - Limits on disclosure of personal information
Principle 12 - Special restrictions on disclosure of personal information

Those principles are modified by the Privacy Code of Practice for Local Government made by the Attorney General. To date there has been no Health Records and Information Privacy Code of Practice made for Local Government.

The Privacy Code has been developed to enable Local Government to fulfil its statutory duties and functions under the *Local Government Act 1993* (LGA) in a manner that seeks to comply with the PPIPA.

This Plan outlines how the Council will incorporate the 12 Information Protection Principles into its everyday functions.

This Plan should be read in conjunction with the Code of Practice for Local Government.

Nothing in this Plan is to:

- Affect any matter of interpretation of the Codes or the Information Protection Principles and the Health Privacy Principles as they apply to the Council.
- Affect any obligation at law cast upon the Council by way of representation or holding out in any manner whatsoever.
- Create, extend or lessen any obligation at law which the Council may have.

This Plan is designed to introduce policies and procedures to maximise compliance with the PPIPA and the HRIPA.

Where the Council has the benefit of an exemption, it will nevertheless describe procedures for compliance in this Plan. By doing so, it is not to be bound in a manner other than that prescribed by the Codes.

Council collects, stores and uses a broad range of information. A significant part of that information is personal information. This Plan applies to that part of the Council's information that is personal information.

It may mean in practice that any information that is not personal information will receive treatment of a higher standard; namely treatment accorded to personal information where the information cannot be meaningfully or practicably separated.

1.1 What is "personal information"?

"Personal information" is defined in section 4 of the PPIPA as follows:

Personal information is defined to mean information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This information can be on a database and does not necessarily have to be recorded in a material form.

1.2 What is not "personal information"?

"Personal information" does not include "information about an individual that is contained in a publicly available publication". Personal information, once it is contained in a publicly available publication, ceases to be covered by the PPIPA.

Section 4A of the PPIPA also specifically excludes "health information", as defined by section 6 of the HRIPA, from the definition of "personal information", but includes "health information" in the PPIPA's consideration of public registers (discussed below). "Health information" is considered in Part 4 of this Plan.

Where the Council is requested to provide access or make a disclosure and that information has already been published, then the Council will rely on the provisions of the relevant Act that authorises Council to hold that information and not the PPIPA (for example, section 8 of the *Government Information (Public Access) Act 2009* (GIPA Act).

Council considers the following to be publicly available publications:

- An advertisement containing personal information in a local, city or national newspaper.
- Personal information on the Internet.
- Books or magazines that are printed and distributed broadly to the general public.
- Council Business papers or that part that is available to the general public.
- Personal information that may be a part of a public display on view to the general public.

Information published in this way ceases to be covered by the PPIPA.

Council's decision to publish in this way must be in accordance with PPIPA.

1.3 Policy on Electoral Rolls

The Electoral Roll is a publicly available publication. Council will refer any requests for access to or copies of the Electoral Roll to the State Electoral Commissioner.

1.4 Application of This Plan

The PPIPA, the HRIPA and this Plan apply, wherever practicable, to:

- Councillors
- Council employees
- Volunteers
- Consultants and contractors of the Council
- Council owned businesses
- Council committees (including community members of those committees which may be established under section 355 of the LGA).

Council will ensure that all such parties are made aware that they must comply with the PPIPA, the HRIPA, any other applicable Privacy Code of Practice and this Plan.

1.5 Personal Information Held by Council

The Council holds personal information concerning Councillors, such as:

- Personal contact information
- Complaints and disciplinary matters
- Pecuniary interest returns
- Entitlements to fees, expenses and facilities.

The Council holds personal information concerning its customers, ratepayers and residents, such as:

- Rates records
- DA applications and related submissions
- Submissions and information provided as part of community consultation and engagement
- Unsolicited complaints
- Childcare legacy records (pre 2020)
- Library lending records
- Community service utilisation (e.g. Meals on wheels and community transport)
- CCTV vision
- Various types of health information (see under Part 4 for detailed examples).

The Council holds personal information concerning its employees, such as:

- Recruitment material
- Leave and payroll data
- Personal contact information
- Performance management plans
- Disciplinary matters
- Pecuniary interest returns
- Wage and salary entitlements
- Counselling attendance information
- Complaints and disciplinary matters
- Public interest disclosure investigations
- Health information (such medical certificates and workers compensation claims).

The Council holds personal information concerning its volunteers, such as:

- Recruitment material
- Personal contact information
- Expenses reimbursement.

1.6 Applications for Suppression in Relation to General Information (Not Public Registers)

Under section 739 of the LGA a person can make an application to suppress certain material that is available for public inspection in circumstances where the material discloses or would disclose the person's place of living if the person considers that the disclosure would place the personal safety of the person or their family at risk.

Section 739 of the LGA relates to publicly available material other than public registers. As such, it limits disclosure in those circumstances where an application for suppression is successful. An application for suppression must be verified by statutory declaration and otherwise meet the requirements of section 739. When in doubt, Council will err in favour of suppression.

For more information regarding disclosure of information (other than public registers) see the discussion of IPPs 11 and 12 in Part 3 of this Plan. For information regarding suppression of information on public registers, see Part 2 of this Plan.

1.7 Caution as to Unsolicited Information

Where an individual, a group or committee, not established by Council, gives Council unsolicited personal or health information, then that information should be still treated in accordance with this Plan, the Codes, the HRIPA and the PPIPA for the purposes of IPPs 5-12 and HPPs 5-15 which relate to storage, access, use and disclosure of information.

Note that for the purposes of section 10 of the HRIPA, the Council is not considered to have "collected" health information if the receipt of the information by the Council is unsolicited.

Section 4(5) of the PPIPA also provides that personal information is not "collected" by Council if it is unsolicited.

2.0 Public Registers

A public register is defined in section 3 of the PPIPA:

"…public register means a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)."

A distinction needs to be drawn between "public registers" within the meaning of Part 6 of the PPIPA and "non public registers". A "non public register" is a register but it is not a "public register" for the purposes of the PPIPA. For example, the register might not be publicly available or it may not contain personal information.

Disclosure in relation to public registers must comply with Part 6 of the PPIPA and the Privacy Code. Personal information cannot be accessed by a person about another person unless the personal information is contained in a public register.

Where personal information is contained in a public register, then Part 6 of the PPIPA applies to determine whether access to that information will be given to another person.

Disclosure in relation to all other personal information must comply with the Information Protection Principles as outlined in Part 2 of this Plan and the Privacy Code where it includes personal information that is not published.

The Council holds the following public registers:

Name of Register	Act and Section	Purpose of the Register	
		Primary Purpose	**Secondary Purpose**
Property and Land Register. *Available for inspection free of charge.* *Register available for inspection on Council's website*	LGA s53	To identify all land vested in Council, or under its control	Consideration of public accountability as to the land held by Council, so third part access is a secondary purpose
Record of Approvals. *Available for inspection free of charge.* *Register held by Development Services Support Officer*	LGA s113	To identify all approvals granted under the LGA	
Register of Councillor Voting on Planning Decisions *Available for inspection on Council's website*	LGA s375A	To record voting details of each planning decision made under the EPPA at a meeting of the Council or a Council committee.	
Register of Pecuniary Interests. *Available for inspection free of charge.* *Register available for inspection on Council's website* *Personal information is redacted from published returns pursuant to Council's Disclosure of Interests Returns Corporate Practice*	LGA s440AAA (3)-s440AAB Code of Conduct cl4.21	To determine whether or not a Councillor or a member of a council committee has a pecuniary interest in any matter with which the council is likely to be concerned.	Corresponding public accountability purpose and third party access is a secondary purpose.
Rates Register. *Council will not release names and addresses of owners excepting to adjoining owners on proof of ownership for fence development and property issues.* *Council will not sell property details for commercial purposes.* *Register held by Financial Services*	LGA s602	To record the value of a parcel of land and rate liability in respect of that land	Recording the owner or lessee of each parcel of land
Disclosures Log *Available for inspection on Council's website*	GIPA Act s25 and 26	To records details about formal access applications which may be of interest to other members of the public.	

Name of Register	Act and Section	Purpose of the Register	
		Primary Purpose	Secondary Purpose
Register of Government Contracts *Available for inspection on Council's website*	GIPA Act s27	To record information about each government contract to which Council is a party that has (or is likely to have) a value of $150,000 or more.	
Register of Current Declarations of Disclosures of Political Donations to Councillors *Available for inspection on Council's website*	EPA s10.4 (4) and (5)	To record all current donations and expenditure declarations lodged by Councillors with the Election Funding Authority of NSW.	
Register of DA Lodgement. *Available for inspection free of charge.* *Register held by Development Services Support Officer*	EPAA s4.58	To identify applications for development consent	
Integrated Development Assessment Index for Approved Applications. *Available for inspection free of charge.* *Register held by Development Services Support Officer*	EPAA s4.58	To identify applications for other approvals, confirm determinations on appeal and identify applications for complying development certificates	
Record of Building Certificates. *Available for inspection free of charge. Copies of certificate only available with owner/s' consent and payment of prescribed fee.* *Register held by Development Services Support Officer*	EPA s6.26 (8),(9) and(10)	To identify all building certificates	
Public notices issued under the Act. *Available for inspection free of charge.* *Register held by Department Environment and Planning*	POEOA s91	To identify all public notices issued under the POE Act	
Public register of licences held. *Available for inspection free of charge.* *Register held by Development Services Support Officer*	POEOA s308	To identify all licences granted under the Act	
Record of all property taken into possession. *Available for inspection free of charge.* *Register held by Compliance*	PSUPA s33 and PSUPR s18	To identify all property taken possession of by authorised officers and how it was dealt with.	

LGA	*Local Government Act 1993*
GIPA	*Government Information (Public Access) Act 2009*

EPAA	*Environmental Planning and Assessment Act 1979*
POEOA	*Protection of the Environment Operations Act 1997*
PSUPA	*Public Spaces (Unattended Property) Act 2021*
PSUPR	*Public Spaces (Unattended Property) Regulation 2022*

Members of the public may enquire only in accordance with the primary purpose of any of these registers. The primary purpose for each of these public registers is set out in the sections that follow.

2.1 Public Registers, the PPIPA and the HRIPA

A public register generally confers specific rights or privileges, a benefit, or status, which would not otherwise exist. It may be required by law to be made publicly available or open to public inspection, or it is simply made publicly available or open to public inspection (whether or not payment is required).

Despite the exclusion of "health information" from the definition of "personal information" under section 4A of the PPIPA, section 56A of the PPIPA includes as "personal information", "health information" on public registers.

Section 57 of the PPIPA requires very stringent controls over the disclosure of personal information contained in a public register. It provides broadly that where Council is responsible for keeping a public register, it will not disclose any personal information kept in that register unless it is satisfied that the information is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

Section 57 (2) provides that in order to ensure compliance with section 57(1), a Council may require any person who applies to inspect personal information contained in the public register to give particulars in the form of a statutory declaration as to the proposed use of that information. (Form at Appendix 1 may be used a guide)

Councils also need to consider the Privacy Code of Practice for Local Government which has the effect of modifying the application of Part 6 of the PPIPA (the "public register" provisions).

If the stated purpose of the applicant does not conform with the purpose for which the public register is kept, access to the information sought will not be given.

Where personal information is contained in a publicly available publication, that information will not be regarded as personal information covered by the PPIPA or as health information for the purposes of part 6 of the PPIPA.

2.2 Effect on Section 6 of the GIPA Act

Section 57 of the PPIPA prevails over clause 1(3) of Schedule 1 of the *Government Information (Public Access) Regulation 2009* (GIPA Regulation) to the extent of any inconsistency. Therefore:

1. If a register is listed in Schedule 1 of the GIPA Regulation, access must not be given except in accordance with section 57(1) of the PPIPA.

2. If a register is not listed in Schedule 1 of the GIPA Regulation, access must not be given except:

(i) If it is allowed under section 57(1) of the PPIPA.

(ii) There is no overriding public interest against disclosure of the information under section 6 of the GIPA Act.

Note: Both 1 and 2 are amended with regard to specific public registers in the Privacy Code of Practice for Local Government.

2.3 Where Some Information in the Public Register Has Been Published

That part of a public register that is not published in a publicly available publication will be treated as a "public register" and the following procedure for disclosure will apply.

For example, the Register of Consents and Approvals held by Council under section 4.58 of the *Environmental Planning and Assessment Act 1979* requires Council to advertise or publish applications for development consent.

When Council publishes the address of the property, it may identify the owner. The personal information that has not been published and any applications not advertised or that have been rejected or withdrawn (and hence also not published) will be treated as a public register under PPIPA.

Council may hold a register under the *Contaminated Land Management Act 1997* on behalf of the Environment Protection Authority. This is not to be considered a public register of the Council as the statute does not place any obligations on the Council to make this register publicly available as a register of contaminated land. Furthermore, the legislation foreshadows that the Environment Protection Authority may indeed post this list or register on the internet. This may constitute a publication of the information and therefore the PPIPA will not apply.

Registers should not be published on the internet.

2.4 Disclosure of Personal Information Contained in the Public Registers

A person seeking a disclosure concerning someone else's personal information from a public register must satisfy Council that the intended use of the information is for a purpose relating to the purpose of the register or the Act under which the register is kept.

In the following section, by way of guidance only, what might be called the "primary" purpose (or "the purpose of the register") has been specified for each identified register. In some cases a "secondary purpose" has also been specified, by way of guidance as to what might constitute "a purpose relating to the purpose of the register".

2.5 Purposes of Public Registers

Purposes of public registers under the Local Government Act 1993

Section 53 - Land Register – The primary purpose is to identify all land vested in Council, or under its control. The secondary purpose includes a consideration of public accountability as to the land held by Council. Third party access is therefore a secondary purpose.

Section 113 - Records of Approvals – The primary purpose is to identify all approvals granted under the LGA.

Section 440AAB - Register of Pecuniary Interests – The primary purpose of this register is to determine whether or not a Councillor or a member of a Council committee has a pecuniary interest in any matter with which the Council is likely to be concerned. There is a corresponding public accountability purpose and third party access is a secondary purpose.

Section 602 - Rates Record - The primary purpose is to record the value of a parcel of land and record rate liability in respect of that land. The secondary purpose includes recording the owner or lessee of each parcel of land. For example, that a disclosure on a section 603 (of the LGA) rating certificate that a previous owner was a pensioner is considered to be allowed, because the secondary purpose is “a purpose relating to the purpose of the register”.

Purposes of public registers under the Environmental Planning and Assessment Act 1979

Section 4.58 – Register of consents and approvals – The primary purpose is to identify applications for development consent and other approvals, confirm determinations on appeal and identify applications for complying development certificates.

Section 6.26 (8), (9) and (10) – Record of building certificates – The primary purpose is to identify all building certificates.

Purposes of public registers under the Protection of the Environment (Operations) Act 1997

Section 308 – Public register of licences held – The primary purpose is to identify all licences granted under the Act.

Purposes of the public register under the Public Spaces (Unattended Property) Act 2021 and Public Spaces (Unattended Property) Regulation 2022

Section 33 Act and Section 18 Reg – Record of all property taken possession of and details of how it was dealt with – The primary purpose is to identify all property taken possession of and details of how it was dealt with by Council.
Secondary purpose of all Public Registers

Due to the general emphasis (to be found in the LGA and elsewhere) on local government processes and information being open and accountable, it is considered that a secondary purpose for which all public registers are held by Council includes the provision of access to members of the public. Therefore disclosure of specific records from public registers would normally be considered to be allowable under section 57 of the PPIPA.

However, requests for access, copying or the sale of the whole or a substantial part of a Public Register held by Council will not necessarily fit within this purpose. Council should be guided by the Privacy Code of Practice for Local Government in this respect. Where Council officers have doubt as to the intended use of the information, an applicant may be requested to provide a statutory declaration so that Council may satisfy itself as to the intended use of the information.

Council will make its assessment as to the minimum amount of personal information that is required to be disclosed with regard to any request.

Other Purposes

Persons or organisations who apply to Council to have access to the information contained in any public register for a purpose not related to the purpose of the register, may be given

access at the discretion of Council but only in accordance with the Privacy Code of Practice for Local Government concerning Public Registers.

2.6 Applications for Access to Own Records on a Public Register

A person wishing to have access to a public register to confirm their own details needs only to prove their identity to Council before having access to their own personal information.

2.7 Applications for Suppression in Relation to a Public Register

An application for suppression in relation to a public register will be dealt with under PPIPA, rather than section 739 of the LGA.

A person about whom personal information is contained (or proposed to be contained) in a public register, may request Council under section 58 of the PPIPA to have the information removed from, or not placed on the register.

If Council is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, Council will suppress the information in accordance with the request unless Council is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information, in accordance with section 58(2) of the PPIPA. ("Well-being" is defined in the Macquarie Dictionary as "the good or satisfactory condition of existence; welfare".)

When in doubt, Council will err in favour of suppression.

Any information that is removed from, or not placed on, that aspect of a public register to be made public may be kept on the register for other purposes. That is, the information may still be used for Council functions, but it cannot be disclosed to other parties.
An application for suppression should be made in writing addressed to the General Manager and must outline the reasons for the request. The Council may require supporting documentation where appropriate.

2.8 Other Registers

Council may have other registers that are not public registers. The Information Protection Principles, this Plan, any applicable Codes and the PPIPA apply to those registers or databases.

Access to Information Other Than That Kept on Public Registers

Council requires that an application form be completed for each request for access to personal information. No requests for personal information will be met by telephone. A flow chart is attached at Appendix 7 indicating the decision rule for providing access to personal information.

3.0 The Information Protection Principles

3.1 Information Protection Principle 1 – Section 8

Section 8 Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless:

a) The information is collected for a lawful purpose that is directly related to a function or activity of the agency.
b) The collection of the information is reasonably necessary for that purpose.

(2) A public sector agency must not collect personal information by any unlawful means.

The Privacy Code of Practice for Local Government.

The Code makes no provision to depart from the requirements of this principle.

Council Policy

Council will only collect personal information for a lawful purpose as part of its proper functions. The LGA governs Council's major obligations and functions.

Section 22 of the LGA provides other functions under other Acts. Some of those Acts are as follows:

- *Community Land Development Act 2021*
- *Companion Animals Act 1998***
- *Conveyancing Act 1919*
- *Environmental Planning and Assessment Act 1979*
- *Fire and Rescue NSW Act 1989*
- *Fluoridation of Public Water Supplies Act 1957*
- *Food Act 2003*
- *Library Act 1939*
- *Protection of the Environment Operations Act 1997*
- *Public Health Act 2010*
- *Public Spaces (Unattended Property) Act 2021*
- *Recreation Vehicles Act 1983*
- *Roads Act 1993*
- *Rural Fires Act 1997*
- *State Emergency Service Act 1989*
- *Strata SchemesDevelopment Act 2015*
- *Swimming Pools Act 1992*

This list is not exhaustive.

Additionally, the exercise by Council of its functions under the LGA may also be modified by the provisions of other Acts. Some of those Acts follow:

- *Coastal Management Act 2016*
- *Government Information (Public Access) Act 2009*
- *Heritage Act 1977*
- *Privacy and Personal Information Protection Act 1998*
- *State Emergency and Rescue Management Act 1989*
- *Unclaimed Money Act 1995*

The circumstances under which Council may collect information, including personal information, are varied and numerous.

Council will not collect any more personal information than is reasonably necessary for it to fulfil its proper functions.

Anyone engaged by Council as a private contractor or consultant that involves the collection of personal information must agree to be bound not to collect personal information by any unlawful means. This will include debt recovery actions by or undertaken on behalf of Council by commercial agents.

***Companion Animals Act*

Collection of information under the *Companion Animals Act* and Council's use of the Companion Animals Register should be guided by the Office of Local Government's guidelines, which have been developed with the PPIPA in mind.

Role of the Privacy Contact Officer

In order to ensure compliance with Information Protection Principle 1, internet contact forms, rates notices, application forms of whatsoever nature, or written requests by which personal information is collected by Council; will be referred to the Privacy Contact Officer prior to adoption or use.

The Privacy Contact Officer will also provide advice as to:

1. Whether the personal information is collected for a lawful purpose
2. If that lawful purpose is directly related to a function of Council
3. Whether or not the collection of that personal information is reasonably necessary for the specified purpose.

Any further concerns of a legal nature will be referred to Council's solicitor.

3.2 Information Protection Principle 2 – Direct Collection

Section 9 Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

a) The individual has authorised collection of the information from someone else, or

b) In the case of information relating to a person who is under the age of 16 years - the information has been provided by a parent or guardian of the person.

The Privacy Code of Practice for Local Government

The Code makes provision for Council to depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.

Council Policy

The compilation or referral of registers and rolls are the major means by which the Council collects personal information. For example, the information the Council receives from the Land Titles Office would fit within section 9(a) above.

Other means include forms that customers may complete and lodge with Council for development consent, companion animal registration, applications for specific inspections or certifications or applications in respect of tree preservation orders.

In relation to petitions, the Council will treat the personal information contained in petitions in accordance with PPIPA.

Where Council or a Councillor requests or requires information from individuals or groups, that information will be treated in accordance with PPIPA.

Information Collected as a Result of a Community Engagement Process

Council engages the public by way of public meetings, surveys or invitation for submissions in relation to Council proposals or applications made to Council. Council advises the public in notification letters, notices, newsletters and the like, on the website, in the local press, and at public meetings how any personal information that is collected will be handled.

Personal information collected at public meetings will only be collected for the purpose of ongoing consultation on the issue or associated issues by Council officers. Such information will not be made available for release to the public. All submissions received as part of a community engagement process will be considered in the public arena and any such submission will be made available for release to the public.

The name and address of persons who address Council and Committee meetings will be recorded in the Minutes of the meetings which become publicly available including publication on Council's website.

Council regards all information concerning its customers as information protected by PPIPA. Council will therefore collect all personal information directly from its customers except as provided in section 9 or under other statutory exemptions or Codes of Practice. Council may collect personal information from other public sector agencies in respect of specific statutory obligations where it is authorised by law to do so.

Where Council anticipates that it may otherwise need to collect personal information indirectly it will first obtain the authorisation of each individual under section 9 (a) of the PPIPA.

External and Related Bodies

Each of the following will be required to comply with this Plan, any applicable Privacy Code of Practice, and the PPIPA:

- Council owned businesses
- Council consultants
- Private contractors
- Council committees

Council will seek to contractually bind each of these bodies or persons to comply with the PPIPA.

Where any of the above collects personal information on behalf of Council or in relation to the performance of their activities, that body or person will be required to:

- Obtain a written authorisation and consent to that collection; and
- Notify those persons in accordance with information protection principle 3 as to the intended recipients and other matters required by that principle.

Council owned businesses, committees and private contractors or consultants must abide by this Plan, the Code and the PPIPA under the terms of their incorporation by Council or by contract.

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 2.

Existing statutory exemptions under the Act

Compliance with Information Protection Principle 2 is also subject to certain exemptions under the Act. If one of those exemptions applies, Council need not comply. The statutory exemption will be relied upon only in very obvious and limited circumstances and legal advice should normally be obtained.

The relevant statutory exemptions follow:

Section 23(2) of the PPIPA permits non-compliance with Information Protection Principle 2 if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal.

Section 24(4) of the PPIPA extends the operation of section 24(1) to councils and permits non-compliance with Information Protection Principle 2 if a Council is:

(i) Investigating or otherwise handling a complaint or other matter that could be referred or made to, or has been referred from or made by, an investigative agency; and

(ii) If compliance might detrimentally affect (or prevent the exercise of) the Council's complaint handling or investigative functions.

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 2 where the agency is lawfully authorised or required not to comply with the principle.

(iii) Section 25(b) of the PPIPA permits non-compliance with Information Protection Principle 2 where non-compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Section 26(1) of the PPIPA permits non-compliance with Information Protection Principle 2 if compliance would prejudice the interests of the individual concerned.

Further Explanation regarding IPP 2

Where Council cannot collect personal information directly from the person, it will ensure one of the following:

1. Council has obtained authority from the person under section 9(a) of the PPIPA.

2. The collection of personal information from a third party is permitted under an Act or law. (For example, the indirect collection from the Land Titles Office).

3. The collection of personal information from a parent or guardian is permitted provided the person is less than 16 years of age.

4. The collection of personal information indirectly where one of the above exemptions applies.

5. The collection of personal information indirectly is permitted under the Privacy Code of Practice for Local Government or the Investigative Code of Practice.

Code of Practice for Local Government or the Investigative Code of Practice

The only other exception to the above is in the case where Council is given unsolicited information.

3.3 Information Protection Principle 3 - Requirements when Collecting Personal Information

Section 10 Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

a) The fact that the information is being collected

b) The purposes for which the information is being collected

c) The intended recipients of the information

d) Whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided

e) The existence of any right of access to, and correction of, the information

f) The name and address of the agency that is collecting the information and the agency that is to hold the information

The Privacy Code of Practice for Local Government

The Code makes provision for Council to depart from this principle where personal information is collected about an individual for the purpose of conferring upon that person, an award, prize, benefit or similar form of personal recognition without prior or subsequent notification.

Council Policy

Where Council proposes to collect personal information directly from the person, it will inform that person that the personal information is being collected, what is done with that information and who the intended recipients will be.

Council will inform persons if the information is required by law or voluntarily given. Council will also inform individuals which department or section within Council holds their personal information, and of the right to access and correct that information. Council will adapt the general section 10 pre-collection Privacy Notification form as appropriate (See Appendix 2).

The following are examples of application procedures that will require a Privacy Notification Form in accordance with section 10:

- Lodging Development Applications;
- Lodging objections to Development Applications;
- Lodging applications for approval under the LGA;
- Any stamps or printed slips that contain the appropriate wording for notification under section 10 (see Appendix 2); and
- When collecting an impounded item. In relation to the Privacy Notification Form that may be attached to a Development Application provided to objectors, it could be stated that objectors have a right to remain anonymous if they so choose. However, should they need to substantiate their objections, anonymous objections may be given less weight (or no weight) in the overall consideration of the Application.

Post - Collection

Where Council collects personal information indirectly from another public sector agency in respect of any one of its statutory functions, it will advise those individuals that it has collected their personal information by including a privacy notification form in the next issue of their rates notice, or otherwise by letter. A common example of the collection of information from another public sector agency is the Land Titles Office. Council receives information as to new ownership changes when property is transferred from one owner to the next. Appendix 3 contains a sample Privacy Notification Form that could be used for post-collection.

External and related bodies

Each of the following will be required to comply with Information Protection Principle 3:

- Council owned businesses
- Council consultants
- Private contractors
- Council committees

Council will seek to contractually bind each of these bodies or persons to comply with the Information Protection Principle 3.

Where any of the above collect personal information on behalf of Council or in relation to the performance of their activities, that body or person will be required to notify those persons in accordance with Information Protection Principle 3 as to the intended recipients and other matters required by that principle.

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 3.

Existing Statutory Exemptions under the Act

Compliance with Information Protection Principle 3 is also subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

The relevant statutory exemptions follow:

Section 23(3) permits non-compliance with Information Protection Principle 3 where information is collected for law enforcement purposes. Law enforcement means a breach of the criminal law and criminal law enforcement. This section does not remove the rights of an accused person.

Section 24(4) of the PPIPA extends the operation of section 24(1) to councils and permits non-compliance with Information Protection Principle 3 if a Council is:

(i) Investigating or otherwise handling a complaint or other matter that could be referred or made to, or has been referred from or made by, an investigative agency; and

(ii) If compliance might detrimentally affect (or prevent the exercise of) the Council's complaint handling or investigative functions.

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 3 where the agency is lawfully authorised or required not to comply with the principle.

Section 25(b) of the PPIPA permits non-compliance with Information Protection Principle 3 where non-compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Section 26(1) of the PPIPA permits non-compliance with Information Protection Principle 3 if compliance would prejudice the interests of the individual concerned.

Section 26(2) of the PPIPA permits non-compliance where the person expressly consents to such non-compliance.

Disclosure of Information of Research Purposes

The disclosure of personal information for research purposes will be allowed only in accordance with any applicable Direction made by the Privacy Commissioner under section 41 of PPIPA or any Research Code of Practice made by the Attorney General as may be in force for the time being.

3.4 Information Protection Principle 4 - Other Requirements Relating to Collection of Personal Information

Section 11 Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

a) The information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete

b) The collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Council Policy

Council will seek to ensure that no personal information is collected which is not directly relevant to its proper functions.

Council collects personal information through the various forms that customers may complete and lodge with Council. Before adoption of a new form, a draft form will be reviewed for compliance with Information Protection Principle 4 by the EEO Officer, Council's solicitor, Public Officer or other suitable person. Should Council have any residual doubts, the opinion of the Office of the Privacy Commissioner NSW will be sought.

3.5 Information Protection Principle 5 - Retention and Security of Personal Information

Section 12 Retention and security of personal information

A public sector agency that holds personal information must ensure:

a) That the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

b) That the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and

c) That the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

d) That, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Council Policy

Council may comply with this principle by using any or all of the following or similar documents:

- Records and Archives Services Manual
- The Council's Policy on Security of and Access to Misconduct Files
- Council's Internet Security Policy
- Information Technology Security Policy and
- General Records Disposal Schedule for Local Government.

Disclosure of Information of Research Purposes

The disclosure of personal information for research purposes will be allowed only in accordance with any applicable Direction made by the Privacy Commissioner under section 41 of PPIPA or any Research Code of Practice made by the Attorney General as may be in force for the time being.

3.6 Information Protection Principle 6 - Information Held by Agencies

Section 13 Information about personal information held by agencies

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

a) Whether the agency holds personal information, and

b) Whether the agency holds personal information relating to that person, and

c) If the agency holds personal information relating to that person:

(i) The nature of that information, and

(ii) The main purposes for which the information is used, and

(iii) That person's entitlement to gain access to the information.

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Council Policy

Section 13 of the PPIPA requires a council to take reasonable steps to enable a person to determine whether the council holds personal information about them. If Council holds any information about a person, upon request it will advise them the nature of that information, the main purposes for which it is held, and that person's entitlement to access. As a matter of practicality, not every item of personal information, however insignificant, will be capable of ascertainment.

Under section 20(5) of the PPIPA, Information Protection Principle 6 is subject to any applicable conditions or limitations contained in the GIPA Act. Council must consider the relevant provisions of the GIPA Act.

Any person can make application to Council by completing the appropriate form and submitting it to Council. An example is at Appendix 4.

Where Council receives an application or request by a person as to whether Council holds information about them, Council will undertake a search of its records to answer the enquiry. Council may ask the applicant to describe what dealings the applicant has had with Council in order to assist Council to conduct the search.

Council will ordinarily provide a response to applications of this kind within 28 days of the application being made. The fee structure is commensurate to that of the Council's GIPA Act rates structure.

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 6.

Existing Exemptions under the Act

Compliance with Information Protection Principle 6 is also subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 6 where Council is lawfully authorised or required not to comply with the principle.

Section 25(b) of the PPIPA permits non-compliance with Information Protection Principle 6 where non-compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Reporting Matters

The Council will issue a statement to be included on its Web page (if it has one) and in its Annual Report concerning the nature of personal information it regularly collects, the purpose for which the personal information is used and an individual's right to access their own personal information.

3.7 Information Protection Principle 7 - Access to Personal Information Held by Agencies

Section 14 Access to personal information held by agencies

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Council Policy

Section 14 of the PPIPA requires a council, at the request of any person, to give access to that person to personal information held about them.

Compliance with Information Protection Principle 7 does not allow disclosure of information about other people. If access to information that relates to someone else is sought, the application must be made under the GIPA Act, unless Information Protection Principles 11 and 12 or the Public Register provisions apply.

Where a person makes an application for access under the PPIPA and it is involved or complex, it may be referred, with the written consent of the applicant, as an application under the GIPA Act. However use of the GIPA Act is to be a last resort. The applicant has the right to insist on being dealt with under PPIPA.

Under section 20(5) of the PPIPA, Information Protection Principle 7 is subject to any applicable conditions or limitations contained in the GIPA Act. Council must consider the relevant provisions of the GIPA Act.

Customers wishing to exercise their right of access to their own personal information should apply in writing or direct their inquiries to the General Manager, who will make a determination. A sample form is provided at Appendix 5.

Members of staff wishing to exercise their right of access to their personal information should apply in writing on the attached form or direct their inquiries to the Manager of Personnel, who will deal with the application.

In order to comply with the requirement to provide the requested information "without excessive delay or expense", Council will ordinarily provide a response to applications of this kind within 28 days of the application being made.

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 7.

Existing Exemptions under the Act

Compliance with Information Protection Principle 7 is also subject to certain exemptions under the Act. If one of those exemptions applies, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 7 where Council is lawfully authorised or required not to comply with the principle.

Section 25(b) of the PPIPA non-compliance with Information Protection Principle 7 where non-compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

3.8 Information Protection Principle 8 - Alteration of Personal Information

Section 15 Alteration of personal information

(1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

a) Is accurate, and

b) Having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

(4) This section, and any provision of privacy code of practice that relates to the requirements set out in this section, apply to public sector agencies despite section 25 of this Act and section 21 of the *State Records Act 1998*.

(5) The Privacy Commissioner's guidelines under section 36 may make provision for or with respect to requests under this section, including the way in which such a request should be made and the time within which such a request should be dealt with.

(6) In this section (and in any other provision of this Act in connection with the operation of this section), public sector agency includes a Minister and a Minister's personal staff.

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Council Policy

Section 15 of the PPIPA allows a person to make an application to Council to amend (this includes by way of corrections, deletions or additions) personal information held about them so as to ensure the information is accurate, and, having regard to the purpose for which the information is collected, relevant to that purpose, up to date and not misleading.

Council wishes to have its information current, accurate and complete. Proposed amendments or changes to the personal information held by the Council are welcomed.

If Council declines to amend personal information as requested, it will on request of the individual concerned, place an addendum on the information in accordance with section 15(2) of the PPIPA.

Where there are complaints that are or could be the subject of a staff complaint or grievance, they will be referred to the Manager Personnel in the first instance and treated in accordance with the "Grievance and Complaint Handling Procedures".

Any alterations that are or could be the subject of a customer complaint or grievance will be referred to the General Manager, who will make a determination in relation to the matter.

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 8.

Existing Exemptions under the Act

Compliance with Information Protection Principle 8 is also subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 8 where Council is lawfully authorised or required not to comply with the principle.

Section 25(b) of the PPIPA permits non-compliance with Information Protection Principle 8 where non-compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Procedure

Where information is requested to be amended (either by way of correction, deletion or addition), the individual to whom the information relates must make a request.

That request should be accompanied by appropriate evidence as to the cogency of the making of the amendment, sufficient to satisfy the Council that the proposed amendment is factually correct and appropriate. The Council may require further documentary evidence to support certain amendments. Council will not charge to process an application to amend a record under section15.

The Council's application form for alteration under IPP 8 is at Appendix 6 at the end of this Plan.

Where Council is Not Prepared to Amend

If the Council is not prepared to amend the personal information in accordance with a request by the individual the Council may attach to the information in such a manner as is capable of being read with the information, any statement provided by that individual.

Where an Amendment is Made

If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have the recipients of that information notified of the amendments made by the Council. The Council will seek to notify recipients of information as soon as possible, of the making of any amendment, where it is reasonably practicable.

State Records Act

The *State Records Act* does not allow for the deletion of records. However, as a result of section 20(4) of the PPIPA, some deletions may be allowed in accordance with Information Protection Principle 8.

3.9 Information Protection Principle 9 – Agency Must Check Accuracy of Personal Information before Use

Section 16 Agency must check accuracy of personal information before use

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Council Policy

The steps taken to comply with section 16 will depend on the age of the information, its likelihood of change and the particular function for which the information was collected.

The more significant the information, the greater the necessity that checks to ensure its accuracy and currency be undertaken prior to its use.

For example, each employee's record should be updated when there is any change of circumstances or when the employee's contact details change.

3.10 Information Protection Principle 10 - Limits On Use of Personal Information

Section 17 Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

a) The individual to whom the information relates has consented to the use of the information for that other purpose, or

b) The other purpose for which the information is used is directly related to the purpose for which the information was collected, or

c) The use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

The Privacy Code of Practice for Local Government

The Code makes provision that Council may use personal information for a purpose other than the purpose for which it was created in the following circumstances:

(i) Where the use is in pursuance of Council's lawful and proper function/s and Council is satisfied that the personal information is reasonably necessary for the exercise of such function/s; or

(ii) Where personal information is to be used for the purpose of conferring upon a particular person, an award, prize, benefit or similar form of personal recognition.

Explanatory Note

Council may use personal information obtained for one purpose for another purpose in pursuance of its lawful and proper functions. For example, the Rates Record that Council holds under section 602 of the LGA may also be used to:

- Notify neighbours of a proposed development;
- Evaluate a road opening; or
- Evaluate a tree preservation order.

Council Policy

Council will seek to ensure that information collected for one purpose will be used for that same purpose. Where Council may need to use personal information collected for one purpose for another purpose, it will first gain the consent of the individual concerned, unless an exemption applies.

External and Related Bodies

Each of the following will be required to comply with the Information Protection Principle 10:

- Council owned businesses;
- Council consultants;

- Private contractors; and
- Council committees.

Council will seek to contractually bind each of these bodies or persons to comply. Where any of the above seek to use personal information collected for one purpose, that body or person will be required to obtain the written consent of those persons in accordance with section 17(a) to the use of the information for another purpose.

The form of consent should include the following elements:

(1) Insert full name

(2) Insert address

(3) Insert council name information protection act 1998 to (3): hereby consent under section 17(a) of the privacy and personal

(4) Insert name of collecting body/person using the information collected from me by (4)

(5) Insert purpose/s info was collected for the purpose of (5)

Signature Name to be printed

Date signed / /

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 10.

Existing Exemptions under the Act

Compliance with Information Protection Principle 10 is also subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 23(4) of the PPIPA permits Council not to comply with Information Protection Principle 10 where the use of the information for another purpose is reasonably necessary for law enforcement purposes or for the protection of the public revenue.

Law enforcement purposes means a breach of the criminal law and criminal law enforcement. This section does not remove the rights of an accused person. Protection of the public revenue means a fraud with respect to taxes or other revenue earning processes such as avoidance of stamp duty.

Section 24(4) of the PPIPA extends the operation of section 24(2) to councils and permits non-compliance with Information Protection Principle 10 if a council is:

(i) Investigating or otherwise handling a complaint or other matter that could be referred or made to, or has been referred from or made by, an investigative agency; and

(ii) The use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in order to enable the council to exercise its complaint handling functions or any of its investigative functions.

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 10 where Council is lawfully authorised or required not to comply with the principle.

Section 25(b) of the PPIPA permits non-compliance with Information Protection Principle 10 where non-compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Section 28(3) of the PPIPA permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government (e.g., the Office of Local Government) or a public sector agency under the administration of the Premier for the purpose of informing the Minister (or Premier) about any matter within the Minister's (or Premier's) administration.

3.11 Information Protection Principle 11 - Limits on Disclosure of Personal Information

Section 18 Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

a) The disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or

b) The individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or

c) The agency 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 concerned or another person.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

The Privacy Code of Practice for Local Government

The Code makes provision for Council to depart from this principle in the circumstances described below:

(1) Council may disclose personal information to public sector agencies or public utilities on condition that:

(i) The agency has approached Council in writing;

(ii) Council is satisfied that the information is to be used by that agency for the proper and lawful function/s of that agency, and

(iii) Council is satisfied that the personal information is reasonably necessary for the exercise of that agency's function/s.

(2) Where personal information which has been collected about an individual is to be disclosed for the purpose of conferring upon that person, an award, prize, benefit or similar form of personal recognition.

(3) Where Council is requested by a potential employer, it may verify that a current or former employee works or has worked for Council, the duration of that work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

Council Policy

Council will not disclose the information to another person or other body, unless the disclosure is directly related to the purpose for which the information was collected or where the Council has no reason to believe that the individual concerned would object to the disclosure.

Council may disclose personal information to another person or other body where this disclosure is directly related to the purpose for which the personal information was collected and the individual concerned is reasonably likely to have been aware, (or has been made aware in accordance with section 10), of the intended recipients of that information. "Directly related" can mean the disclosure to another person or agency to deliver a service which supplements that of Council or disclosure to a consultant for the purpose of assessing or reviewing the delivery of a program to which the original collection relates.

The council may disclose personal information to another person or other body where this disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

Public Registers

Sections 18 and 57 of the PPIPA should be read in conjunction in regard to Public Registers. Public Registers are discussed further in Part 2 of this Plan.

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 11.

Existing Exemptions under the Act

Compliance with Information Protection Principle 11 is also subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 23(5)(a) of the PPIPA permits non-compliance with Information Protection Principle 11 where disclosure is made to a law enforcement agency in connection with proceedings

for an offence or for law enforcement purposes. Law enforcement purposes means a breach of the criminal law and criminal law enforcement. However Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(b) of the PPIPA permits non-compliance with Information Protection Principle 11 where the disclosure is made to a law enforcement agency for the purpose of ascertaining the whereabouts of a person reported to be missing. However Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(c) of the PPIPA permits non-compliance with Information Protection Principle 11 where disclosure is authorised by subpoena, search warrant or other statutory instrument. However Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(d)(i) of the PPIPA permits non-compliance with Information Protection Principle 11 where disclosure is reasonably necessary for the protection of the public revenue. Protection of the public revenue could mean a fraud with respect to taxes or other revenue earning processes such as avoidance of stamp duty. However Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(d)(ii) of the PPIPA permits non-compliance with Information Protection Principle 11 where disclosure is reasonably necessary to investigate an offence where there are reasonable grounds to believe an offence has been committed.

Section 24(4) of the PPIPA permits non-compliance with Information Protection Principle 11 if:

(i) Investigating a complaint that could be referred or made to, or has been referred from or made by, an investigative agency, and

(ii) If the disclosure is to an investigative agency.

(Note: “investigative agency” is defined at section3 of PPIPA.)

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 11 where Council is lawfully authorised or required not to comply with the principle. Section 25(b) of the PPIPA permits non-compliance with Information Protection Principle 11 where non-compliance is “necessarily implied” or “reasonably contemplated” under any Act or law.

Section 26(2) of the PPIPA permits non-compliance where the person expressly consents to such non-compliance.

Section 28(3) of the PPIPA permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government (e.g. the Office of Local Government) or a public sector agency under the administration of the Premier for the purpose of informing the Minister (or Premier) about any matter within the Minister’s (or Premier’s) administration.

It is anticipated that a disclosure of personal information for research purposes will be allowed under a s.41 Direction made by the Privacy Commissioner until such time as a Research Code of Practice is made by the Attorney General.

Suppression

Information held by Council may be suppressed such as to disallow disclosure that would otherwise be allowed in the circumstances outlined above. See Part 1 of this Plan for more details about suppression of personal information.

3.12 Information Protection Principle 12 - Special Restrictions on Disclosure of Personal Information

Section 19 Special restrictions on disclosure of personal information

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

(2) A public sector agency that holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

a) A relevant privacy law that applies to the personal information concerned is in force in the that jurisdiction or applies to that Commonwealth agency, or

b) The disclosure is permitted under a privacy code of practice.

(3) For the purposes of subsection (2), a relevant privacy law means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.

(4) The Privacy Commissioner is to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales and to Commonwealth agencies.

(5) Subsection (2) does not apply:

a) Until after the first anniversary of the commencement of this section, or

b) Until a code referred to in subsection (4) is made, whichever is the later

The Privacy Code of Practice for Local Government

The Code makes provision for Council to depart from this principle in the circumstances described below:

(1) For the purposes of s.19(2) only, where Council is requested by a potential employer outside New South Wales, it may verify that a current or former employee works or has worked for Council, the duration of that work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

Council Policy

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

Public Registers

Sections 19 and 57 of the PPIPA should be read in conjunction in regard to Public Registers. Public Registers are discussed further in Part 2 of this Plan.

Investigative Functions

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIPA that may affect the application of Information Protection Principle 12.

Existing Exemptions under the Act

Compliance with Information Protection Principle 12 is also subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

The following provisions of the PPIPA permits non-compliance with Information Protection Principle 12:

- Section 23(7) where the disclosure is necessary to investigate an offence or where there are reasonable grounds to believe an offence has been or may be committed.
- Section 25(a) where Council is lawfully authorised or required not to comply with the principle.
- Section 25(b) where non-compliance is “necessarily implied” or “reasonably contemplated” under any Act or law.
- Section 26(2) where the person expressly consents to such non-compliance.
- Section 27A in certain circumstances where information is exchanged between Council and another public sector agency.
- Section 27B for the purposes of research that are in the public interest.
- Section 27D to respond to emergency situations.
- Section 28(3) of the PPIPA permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government (e.g. the Office of Local Government) or a public sector agency under the administration of the Premier for the purpose of informing the Minister (or Premier) about any matter within the Minister’s (or Premier’s) administration.

Suppression

Information held by Council may be suppressed such as to disallow disclosure that would otherwise be allowed in the circumstances outlined above. See Part 1 of this Plan for more details about suppression of personal information.

4.0 Health Privacy Principles

In 2002, most references to 'health information' were taken out of the PPIPA and separate legislation was enacted. The HRIPA was enacted to deal with this specific type of personal information. On and from September 2004, various agencies and organisations, including local councils were expected to comply with the HRIPA in their collection and management of health information.

Health information includes personal information that is information or an opinion about the physical or mental health or a disability of an individual. Health information also includes personal information that is information or an opinion about:

- A health service provided, or to be provided, to an individual
- An individual's express wishes about the future provision of health services to him or her
- Other personal information collected in connection with the donation of human tissue or
- Genetic information that is or could be predictive of the health of an individual or their relatives or descendants.

Health information is defined in section 6 of the HRIPA. Local councils will often hold health information by reason of their role in elder care, child care and various types of community health support services. It is therefore very important for councils to be familiar with the 15 Health Protection Principles ("HPP") set down in Schedule 1 to the HRIPA. Each of these HPPs are considered below.

The following is a non-exhaustive list of examples of the types of health information and circumstances in which councils may collect health information in exercising their functions:

- Tree pruning/removal application where residents approach councils for a reconsideration or reassessment of a tree pruning/removal application on medical grounds
- Issuing of clean up orders which may include recording information about a residents health, GP professional contact details or involvement with mental health services
- Volunteer programs where volunteers are asked to disclose health conditions which may preclude them from some types of volunteer work
- Meals on wheels programs where residents may be asked for medical or dietary requirements, e.g. allergies for catering purposes
- Seniors bus outings where information may be collected on special medical needs
- Councils may provide respite and social support services collecting information that is consistent with the client intake and referral record system
- Information on families for the purposes of children's services. e.g. history of illness, allergies, asthma, diabetes, epilepsy etc.
- Physical exercise classes
- Some councils run Podiatry services
- Information may be collected through a healthy community program
- Children's immunization records and
- Family counsellor/youth support workers records.

HPPs 1-4 concern the collection of health information, HPP 5 concerns the storage of health information, HPPs 6-9 concern the access and accuracy of health information, HPP 10 concerns the use of health information, HPP 11 concerns the disclosure of health information, HPPs 12-13 concern the identifiers and anonymity of the persons to which health information relate, HPPs 14-

15 concern the transferral of health information and the linkage to health records across more than one organisation.

4.1 Health Privacy Principle 1 - Purposes of Collection of Health Information

(1) An organisation must not collect health information unless:

a) The information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and

b) The collection of the information is reasonably necessary for that purpose.

(2) An organisation must not collect health information by any unlawful means.

4.2 Health Privacy Principle 2 - Information Must be Relevant, Not Excessive, Accurate and Not Intrusive

An organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

a) The information is collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and

b) The collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

4.3 Health Privacy Principle 3 - Collection to be From Individual Concerned

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

4.4 Health Privacy Principle 4 - Individual to be Made Aware of Certain Matters

(1) An organisation that collects health information about an individual from the individual must, at or before the time it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following:

a) The identity of the organisation and how to contact it

b) The fact that the individual is able to request access to the information

c) The purposes for which the information is collected

d) The persons to whom (or the type of persons to whom) the organisation usually discloses information of that kind

e) Any law that requires the particular information to be collected

f) The main consequences (if any) for the individual if all or part of the information is not provided

(2) If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is generally aware of the matters listed in subclause (1) except to the extent that:

a) Making the individual aware of the matters would impose a serious threat to the life or health of any individual, or

b) The collection is made in accordance with guidelines issued under subclause (3).

(3) The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).

(4) An organisation is not required to comply with a requirement of this clause if:

a) The individual to whom the information relates has expressly consented to the organisation not complying with it or,

b) The organisation is lawfully authorised or required not to comply with it, or

c) Non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under any Act or any other law including the *State Records Act 1998*), or

d) Compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or

e) The information concerned is collected for law enforcement purposes or,

f) The organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

(5) If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause (1), the organisation must take steps that are reasonable in the circumstances, to ensure that any authorised representative of the individual is aware of those matters.

(6) Subclause (4) (e) does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a compliant or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Council Policy

Council will only collect health information for a lawful purpose that is directly related to Council's activities and is necessary for that purpose (HPP 1).

Council will ensure that the health information is relevant, accurate, up to date and not excessive and that the collection is not unnecessarily intrusive into the personal affairs of the individual (HPP 2).

Council will only collect health information directly from the individual that the information concerns, unless it is unreasonable or impractical for Council to do so. (HPP 3).

Council will tell the person why the health information is being collected, what will be done with it, who else might see it and what the consequences are if the person decides not to provide it. Council will also tell the person how he or she can see and correct the health information.

If Council collects health information about a person from someone else, Council will take reasonable steps to ensure that the subject of the information is aware of the above points (HPP 5).

4.5 Health Privacy Principle 5 - Retention and Security

(1) An organisation that holds health information must ensure that:

a) The information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

b) The information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and

c) The information is protected, by taking such security safeguards as are reasonable in the circumstances against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

d) If it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of an organisation is done to prevent the unauthorised use or disclosure of the information.

Note. Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

(2) An organisation is not required to comply with a requirement of this clause if:

a) The organisation is lawfully authorised or required not to comply with it, or

b) Non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

(3) An investigative agency is not required to comply with subclause (1)(a).

Council Policy

Council will store health information securely and protect health information from unauthorised access, use or disclosure. Health information will not be kept for any longer than is necessary and will be disposed of appropriately (HPP 5).

4.6 Health Privacy Principle 6 - Information about Health Information Held By Organisations

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable, to enable any individual to ascertain:

a) Whether the organisation holds health information, and

b) Whether the organisation holds health information relating to that individual, and

c) If the organisation holds health information relating to that individual:

(i) The nature of that information, and

(ii) The main purposes for which the information is used, and

(iii) That person's entitlement to request access to the information.

(2) An organisation is not required to comply with a provision of this clause if:

a) The organisation is lawfully authorised or required not to comply with the provision concerned, or

b) Non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under any Act or any other law (including the *State Records Act 1998*).

4.7 Health Privacy Principle 7 - Access to Health Information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

Note. Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Access to health information held by public sector agencies may also be available under the *GIPA Act* or the *State Records Act 1998*.

(2) An organisation is not required to comply with a provision of this clause if:

a) The organisation is lawfully authorised or required not to comply with the provision concerned, or

b) Non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

4.8 Health Privacy Principle 8 - Amendment of Health Information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information:

a) Is accurate, and

b) Having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the individual to whom the information relates, the organisation must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.

Note: Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Amendment of health information held by public sector agencies may also be able to be sought under the *PPIPA*.

(4) An organisation is not required to comply with a provision of this clause if:

a) The organisation is lawfully authorised or required not to comply with the provision concerned, or

b) Non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

4.9 Health Privacy Principle 9 - Accuracy

An organisation that holds health information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate,up to date, complete and not misleading.

Council Policy

Council will provide details about what health information Council is holding about an individual and with information about why Council is storing that information and what rights of access the individual has (HPP 6).

Council will allow the individual to access his or her health information without reasonable delay or expense (HPP 7).

Council will allow the individual to update, correct or amend his or her health information where necessary (HPP 8).

Council will make sure that the health information is relevant and accurate before using it (HPP 9).

4.10 Health Privacy Principle 10 -Limits on Use of Health Information

(1) An organisation that holds health information must not use the information for a purpose (a **secondary purpose**) other than the purpose (the **primary purpose**) for which it was collected unless:

a) Consent
The individual to whom the information relates has consented to the use of the information for that secondary purpose, or

b) Direct relation
The secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose or,

Note: For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

b1) Emergency
The use of the information for the secondary purpose meets the following conditions:

(i) The secondary purpose is to assist in a stage of an emergency,

(ii) The use of the information is reasonably necessary to assist in the stage of the emergency,

(iii) It is impracticable or unreasonable for the organisation to seek the consent of the individual to whom the information relates to the use of the information for the secondary purpose, or

c) Serious threat to health or welfare
The use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) A serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) A serious threat to public health and safety, or

c1) Genetic Information
The information is genetic information and the use of the information for the secondary purpose:

(i) Is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates, and

(ii) Is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

d) Management of health services
The use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:
(i) Either:

A. That purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

B. Reasonable steps are taken to de-identify the information, and

(ii) If the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) The use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

e) Training

The use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) Either:

A. That purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

B. Reasonable steps are taken to de-identify the information, and

(ii) If the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) The use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

f) Research

The use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) Either:

A. That purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

B. Reasonable steps are taken to de-identify the information, and

(ii) If the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) The use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purpose of this paragraph, or

g) Find missing person
The use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

h) Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline
The organisation:

(i) Has reasonable grounds to suspect that:

A. Unlawful activity has been or may be engaged in, or

B. A person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW),* or

C. An employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) Uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

i) Law enforcement
The use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

j) Investigative agencies
The use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

k) Prescribed circumstances
The use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:

a) The organisation is lawfully authorised or required not to comply with the provision concerned, or

b) Non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

a) To another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

b) To any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(4A) If health information is used under subclause (1)(b1), the organisation:

(a) Must not hold the information for longer than 18 months, unless extenuating circumstances apply or consent has been obtained, and

(b) If the organisation is a law enforcement agency—must not use the information for the purpose of prosecuting an offence.

(5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Council policy

Council will only use the health information for the purpose for which it was collected or for a directly related purpose that the individual to whom the information relates would expect. Otherwise, Council will obtain the individual's consent (HPP 10).

4.11 Health Privacy Principle 11 – Limits on Disclosure of Health Information

(1) An organisation that holds health information must not disclose the information for a purpose (a **secondary purpose**) other than the purpose (the **primary purpose**) for which it was collected unless:

a) Consent
The individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or

b) Direct relation
The secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or
Note: For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

b1) Emergency
The disclosure of the information for the secondary purpose meets the following conditions—

(i) The secondary purpose is to assist in a stage of an emergency,

(ii) The disclosure of the information is reasonably necessary to assist in the stage of the emergency,

(iii) It is impracticable or unreasonable for the organisation to seek the consent of the individual to whom the information relates to the disclosure of the information for the secondary purpose, or

c) Serious threat to health or welfare
the disclosure of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) A serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) A serious threat to public health or public safety, or

c1) Genetic information
The information is genetic information and the disclosure of the information for the secondary purpose—

(i) Is to a genetic relative of the individual to whom the genetic information relates, and

(ii) Is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates, and

(iii) Is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

d) Management of health services
The disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) Either:

A. That purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

B. Reasonable steps are taken to de-identify the information, and

(ii) If the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) The disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

e) Training

The disclosure of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) Either:

A. That purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

B. Reasonable steps are taken to de-identify the information, and

(ii) If the information could reasonably be expected to identify the individual, the information is not made publicly available, and

(iii) The disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

f) Research

The disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) Either:

A. That purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

B. Reasonable steps are taken to de-identify the information, and

(ii) The disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained, and

(iii) The disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

g) Compassionate reasons

The disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:

(i) The disclosure is limited to the extent reasonable for those compassionate reasons, and

(ii) The individual is incapable of giving consent to the disclosure of the information, and

(iii) The disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and

(iv) If the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information, or

h) Finding missing person
The disclosure of the information for the secondary purpose is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

i) Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline

The organisation:

(i) Has reasonable grounds to suspect that:

A. Unlawful activity has been or may be engaged in, or

B. A person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW),* or

C. An employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) Discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

j) Law enforcement
The disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

k) Investigative agencies
The disclosure of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

l) Prescribed circumstances
The disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

2. An organisation is not required to comply with a provision of this clause if:

a) The organisation is lawfully authorised or required not to comply with the provision concerned, or

b) Non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

c) The organisation is an investigative agency disclosing information to another investigative agency.

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

a) To another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

b) To any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) If health information is disclosed in accordance with subclause (1), the person, body or organisation to whom it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(5A) If health information is disclosed under subclause (1)(b1), the organisation—

(a) Must not hold the information for longer than 18 months, unless extenuating circumstances apply or consent has been obtained, and

(b) If the organisation is a law enforcement agency—must not use the information for the purpose of prosecuting an offence.

(6) The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Council Policy

Council will only disclose health information under the following circumstances:

- With the consent of the individual to whom the information relates; or
- For the purpose for which the health information was collected or a directly related purpose that the individual to whom it relates would expect; or
- If an exemption applies (HPP 11).

4.12 Health Privacy Principle 12 - Identifiers

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

a) The individual has consented to the adoption of the same identifier, or

b) The use or disclosure of the identifier is required or authorised by or under law.

(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

a) The use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)-(k) or 11 (1) (c)-(l), or

b) The individual has consented to the use or disclosure, or

c) The disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:

a) Adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or

b) Use or disclose an identifier of the individual that has been assigned by the public sector agency.

Council Policy

Council will only give an identification number to health information if it is reasonably necessary for Council to carry out its functions effectively (HPP 12).

4.13 Health Privacy Principle 13 - Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

Council Policy

Council will provide health services anonymously where it is lawful and practical (HPP 13).

4.14 Health Privacy Principle 14 - Transborder Data Flows and Data Flow To Commonwealth Agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

a) The organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or

b) The individual consents to the transfer, or

c) The transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or

d) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or

e) All of the following apply:

(i) The transfer is for the benefit of the individual

(ii) It is impracticable to obtain the consent of the individual to that transfer

(iii) If it were practicable to obtain such consent, the individual would be likely to give it, or

f) The transfer is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) A serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) A serious threat to public health or public safety, or

g) The organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or

h) The transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

Council Policy

Council will only transfer personal information out of New South Wales if the requirements of Health Privacy Principle 14 are met.

4.15 Health Privacy Principle 15 - Linkage of Health Records

(1) An organisation must not:

a) Include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or

b) Disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) An organisation is not required to comply with a provision of this clause if:

a) The organisation is lawfully authorised or required not to comply with the provision concerned, or

b) Non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

c) The inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

(3) In this clause:

Health record means an ongoing record of health care for an individual. health records linkage system means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records,and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

Council Policy

Council will only include health information in a system to link health records across more than one organisation if the individual to whom the health information relates expressly consents to the link (HPP 15).

5.0 Implementation of the Privacy Management Plan

5.1 Training Seminars/Induction

During induction, all employees should be made aware that the performance management system has the potential to include personal information on their individual work performance or competency.

Councillors, all staff of the Council including staff of council businesses, members of Council committees, volunteers and contractors should be acquainted with the general provisions of the PPIPA, the HRIPA and in particular, the 12 Information Protection Principles (IPPs), the 15 Health Privacy Principles (HPPs), the Public Register provisions, the Privacy Code of Practice for Local Government, this Plan and any other applicable Code of Practice.

To assist in achieving the privacy principles and the Plan requirements, Council provides a privacy e-learning module for use by staff and has prepared privacy guidelines that have been referred to all staff and provided at induction and refresher programs.

Training and awareness is also addressed as part of the privacy risk governance framework described at clause 8 of the Plan.

5.2 Responsibilities of the Privacy Contact Officer

It is assumed that the Public Officer within Council will be assigned the role of the Privacy Contact Officer unless the General Manager has directed otherwise. This Council has appointed the Manager Governance as the Privacy Contact Officer.

In order to ensure compliance with PPIPA and the HRIPA, the Privacy Contact Officer will review all contracts and agreements with consultants and other contractors, rates notices, application forms of whatsoever nature, and other written requests by which personal information is collected by Council, to ensure that Council is in compliance with the PPIPA.

Interim measures to ensure compliance with IPP 3 in particular may include the creation of stamps or printed slips that contain the appropriate wording (see Appendices 2 and 3).

The Privacy Contact Officer will ensure Council in its public areas has special provisions for working with computer screens. Computer screens may require:

- Fast screen savers
- Face the computers away from the public or
- Only allow the record system to show one record at a time

Council's electronic databases should also be reviewed to ensure that they contain procedures and protocols to check the accuracy and currency of personal and health information.

The Privacy Contact Officer will also provide opinions within Council as to:

(i) Whether the personal or heath information is collected for a lawful purpose

(ii) If that lawful purpose is directly related to a function of Council; and

(iii) Whether or not the collection of that personal or heath information is reasonably necessary for the specified purpose

Any further concerns of a legal nature will be referred to Council's solicitor.

Should the Council require, the Privacy Contact Officer may assign designated officers as "Privacy Resource Officers", within the larger departments of Council. In this manner the Council may ensure that the information protection principles are more broadly understood and that individual departments have a greater focus on the information protection principles and are directly applied to Council's day to day functions.

The Privacy Contact Officer has a responsibility for leading and reviewing the privacy risk governance framework described at clause 8 of this Plan.

5.3 Distribution of Information to the Public

Council may prepare its own literature such as pamphlets on the PPIPA, HRIPA or it may obtain and distribute copies of literature available from the Office of the Privacy Commissioner NSW.

6.0 Internal Review

6.1 How Does the Process of Internal Review Operate?

Under section 53 of the PPIPA a person (the applicant) who is aggrieved by the conduct of acouncil is entitled to a review of that conduct. An application for internal review is to be made within 6 months of when the person first became aware of the conduct.

The application is to be in writing and addressed to Council's Privacy Contact Officer. The Privacy Contact Officer will appoint a Reviewing Officer to conduct the internal review. The Reviewing Officer must not be substantially involved in any matter relating to the application. The Reviewing Officer must be an employee and suitability qualified.

The review must be completed as soon as is reasonably practicable in the circumstances. If the review is not completed within 60 days of the lodgement, the applicant is entitled to seek external review.

The Council must notify the Privacy Commissioner of an application as soon as practicable after its receipt, keep the Commissioner informed of the progress of the application and inform the Commissioner of the findings of the review and of the action it proposes to take in relation to the application.

The Privacy Commissioner is entitled to make submissions in relation to internal reviews and the council is required to consider any relevant material submitted by the Privacy Commissioner. The Council must provide the Privacy Commissioner with a draft of the council's internal review report to enable the Privacy Commissioner to make a submission.

Council may provide a copy of any submission by the Privacy Commissioner to the applicant.

The Council must notify the applicant of the outcome of the review within 14 days of its determination. A copy of the final review should also be provided to the Privacy Commissioner where it departs from the draft review.

An internal review checklist has been prepared by the Office of the Privacy Commissioner NSW and can be accessed from its website http://www.ipc.nsw.gov.au.

The Privacy Commissioner must be notified of a complaint, briefed on progress and notified of the outcome of an internal review under the PPIPA or HRIPA.

6.2 What Happens After an Internal Review?

If the complainant remains unsatisfied, he/she may appeal to the Administrative Decisions Tribunal which hears the matter afresh and may impose its own decision and can make a range of orders including an award of damages for a breach of an information protection principle or a health privacy principle.

7.0 Other Relevant Matters

7.1 Contracts with Consultants and Other Private Contractors

It is necessary to have specific provisions to protect the Council in any dealings with private contractors.

Privacy statements and clauses are provided in Council's tender specifications, agreements and contract documents. The privacy statements and clauses have a consistent corporate approach requiring external parties sign off on the Council's privacy requirements.

7.2 Use of Online and Externally Hosted Electronic Services

Where websites or software applications hosted externally by a third party are utilised by Council to collect and use personal information for service delivery purposes, users of those websites or applications are notified that whilst Council is regarded as the agency that holds the information, a third party may store the information collected. The notification includes the name of the service provider. Examples of applications used by Council include Wufoo, Trybookings and Survey Monkey.

Where Council offers and accepts online applications on its website for services involving the collection, use, and storage of personal information, Council's privacy statement also notifies users of any third party hosting service including the name of the service provider.

Where Council offers electronic delivery of a service or response to an online application involving the dissemination and transfer of personal information by electronic delivery, users of this online service are notified that by opting for electronic delivery, the user acknowledges and accepts that any personal information included in the application and Council's response to the application is delivered via unsecure communications channel and Council cannot guarantee security of the information. Users are given the choice to opt out of receiving Council response electronically.

7.3 Breach Notification

Data and personal information breaches may occur in a number of ways. Council's adopted IT and Cyber Security Policy provides examples and instruction to Council employees on whom they should inform should they become aware of a potential breach of information security or a breach of privacy policy.

The nominated disclosure officers will assess any potential breach of information security and manage the situation. This may include rectification or mitigation of the consequences of the breach and/or amendment to policy, corporate practice or procedures.

7.4 Mandatory Notification of Data Breach Scheme (MNDB Scheme)

Amendments to Part 6A of the PPIPA commence 28 November 2023 requiring Council to review and update this Plan in compliance with new section 33(2)(c1) setting out the procedures and practices used by Council to ensure compliance with the obligations and responsibilities set out in Part 6A for the MNDB Scheme.

Part 6A of the PPIPA provides that in the event of a suspected data breach (access, disclosure or loss of personal information), Council is required to:

- contain the breach and assess the likely severity of harm to impacted individuals
- notify the NSW Privacy Commissioner as well as impacted individuals, if the breach is likely to result in serious harm to an individual
- issue a public notification, where impacted individuals cannot be identified or where it is not reasonably practical to notify them

Information is held by Council if:

- Council is in possession or control of the information
- the information is contained within a State record in respect of which the agency is responsible under the *State Records Act 1998*

- the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement

Eligible data breaches occur where there is:

- unauthorised access to personal information; or
- unauthorised disclosure of personal information; or
- loss of personal information where unauthorised access / disclosure is likely to occur

AND

A likelihood that such breach would result in serious harm to any of the individuals to whom the information relates

No exception apply to eligible data breaches.

Council will consider the following criteria when expeditiously assessing whether an eligible data breach has occurred within 30 days:

- types and sensitivity of personal information
- whether security measures were in place
- persons to whom the unauthorised access or disclosure was, or could be, made or given
- likelihood those persons intend to cause harm, or could circumvent security measures protecting the information
- the nature of the harm
- any other matters specified in guidelines issued by the Privacy Commissioner

If there are reasonable grounds to believe an eligible data breach has occurred, Council will notify:

- the Information Commissioner (in the approved format and including mandated information)
- affected individuals (including mandated information) and where this is not reasonably practicable, through public notification (published online for at least 12 months)

Council will apply the following exemptions to its notification obligations to affected individuals, where:

- multiple agencies are involved (and another agency has notified)
- notification may prejudice ongoing investigations or certain proceedings
- mitigation action has been taken to avoid serious harm / unauthorised access or disclosure
- there is serious risk of harm to health or safety
- cyber security is comprised

Details of the procedures and practices used by Council to ensure compliance with the obligations and responsibilities set out in Part 6A for the MNDB Scheme are set out in Council's Data Breach Policy (to be adopted).

7.5 Other Notifiable Data Breaches

7.5.1 The Notifiable Data Breaches (NDB) scheme, under the Federal *Privacy Act 1988* establishes a mandatory data breach notification scheme that requires

organisations covered by the Federal Privacy Act to notify individuals likely to be at risk of serious harm due to a data breach. The following provision of the *Privacy Act 1988* applies to Council:

- Tax File Number (TFN) Data Breaches

  As Council collects individual's tax file numbers (TFN), it has an obligation to protect the information by implementing reasonable security safeguards in the circumstances. A TFN data breach occurs where TFN information is lost, or subject to an unauthorised access or disclosure. If the TFN data breach is 'likely to result in serious harm' to any individual, the notification requirements under the NDB scheme will be triggered and Council must contain the breach; evaluate and mitigate the risks; notify both the Australian Privacy Commissioner and the affected individuals by preparing a detailed statement about the TFN breach; and develop a prevention plan to mitigate the risk of future data breaches.

7.5.2 There are two other data breach notification schemes which create responsibilities for Council in certain circumstances:

- Sharing of government sector data

  The *Data Sharing (Government Sector) Act 2015* (DSGS Act) has a data breach notification scheme in respect of sharing of government sector data under the DSGS Act with the NSW Data Analytics Centre, or between other government sector agencies. If Council receives personal or health information under the DSGS Act and becomes aware that privacy legislation has been (or is likely to have been) breached, Council must inform the data provider and the NSW Privacy Commissioner of the breach.

- European Union's General Data Protection Regulation

  The *General Data Protection Regulation* (GDPR) applies to any organisation offering goods or services to, or monitoring the behaviour of, individuals living in the European Union (EU). This may include Council's involvement in international exchanges and participation in friendship agreements. The data breach notification requirements under the GDPR include notification to the relevant EU supervisory authority within 72 hours after having become aware of the breach.

7.6 Confidentiality

The obligation of confidentiality is additional to and separate from that of privacy. Nevertheless, a duty to withhold information lies at the heart of both concepts. Confidentiality attaches to information per se, personal or health information to the person to whom that information relates.

An obligation of confidentiality exists for all employees whether express or implied as a matter of law.

Information which may be confidential is also likely to have a separate and independent obligation attaching to it in the form of privacy and in that regard, a release for the purposes of confidentiality will not suffice for privacy purposes. Two separate releases will be required and, in the case of privacy, the person to whom the information relates will be required to provide the release.

7.7 Misuse of Personal or Health Information

Section 664 of the LGA makes it an offence for anyone to disclose information except in accordance with that section. Whether or not a particular disclosure is made with lawful excuse is a matter that requires legal opinion from case to case.

7.8 Regular Review of the Collection, Storage and Use of Personal or Health Information

The information practices relating to the collection, storage and use of personal or health information will be reviewed by the Council every three (3) years. Any new program initiatives will be incorporated into the review process with a view to ascertaining whether or not those programs comply with the PPIPA.

7.9 Regular Review of Privacy Management Plan

When information practices are reviewed from time to time, the Privacy Management Plan will also be reviewed to ensure that the Plan is up to date.

8.0 Privacy Risk Governance

8.1 Training and awareness

The training and awareness identified at clause 5.1 of this Plan forms part of a training cycle that covers all staff, councillors, committee members, contractors and volunteers.

The training and awareness cycle is documented and maintained by the Privacy Officer. Training and awareness may involve:

- Induction training
- On the job training
- Issue of privacy guidelines
- Mandatory and non-mandatory e-learning modules
- Guidelines and policies accessible on Intranet and by direct email
- Issues and hot topics communicated by newsletter, team meetings, General Manager address to staff, and email broadcast

Training, awareness and refresher activities occur at least annually and will place an emphasis on breach reporting.

8.2 Privacy risk self-assessment

Prior to every periodic review of this Plan, Council conducts a self-assessment of its privacy governance using the Information and Privacy Commission's self-assessment tool to enable Council to:

- assess compliance against key privacy requirements
- promote better practices and enhance compliance
- generate a summary report in the management document detailing current and target agency compliance levels
- more precisely identify risks and areas where improvements are required
- develop comprehensive plans to improve compliance with privacy requirements

This information will assist in informing revision of the privacy governance framework and this Plan.

8.3 Privacy risk assessments

8.3.1 Council conducts privacy risk assessments of key risk areas. These may include but are not limited to:

- Breach of privacy legislation including the MNDB Scheme
- Payment card industry data security standards (PCI DSS) compliance failure
- Access to confidential, sensitive or privileged information for personal gain
- Unauthorised destruction of business records
- Inadequate privacy governance framework resulting in non-compliance, breaches and potential penalties
- Inadequate oversite of privacy activities resulting in penalties, legal action and reputational damage to Council
- Lack of awareness of roles and responsibilities with respect to the privacy governance framework
- Lack of understanding of how to secure private or sensitive information
- Cyber attack and security

8.3.2 Council conducts privacy risk assessments of programs of significance where it is likely privacy risks may impact. The role of the assessments is not a compliance exercise but to improve organisational practice and demonstrate respect for individuals' privacy. These assessments are particularly pertinent to implementation of new IT applications and associated and other processes involving the collection, storage and use of information.

The Council manager responsible for a proposed program involving the collection, storage and use of information is required to complete the Checklist identifying privacy issues. That Checklist is maintained by the Privacy Contact Officer.

Should any of the responses to that Checklist be affirmative, that matter must be referred to the Privacy Contact Officer to conduct a privacy risk assessment of the the proposed program in conjunction with the program's manager.

8.3.3 Council ensures that the outcomes of the privacy risk assessments identify what action is to be taken in the event of a breach or non-compliance and that these actions align with Council's Business Continuity Plan and Sub-Plans.

8.4 Privacy risk register

The completed checklists and privacy risk assessments described in 8.3 are documented in Council's Pricy Risk Register.

Privacy risk assessment also means privacy impact assessment (PIA).

Related Information

Business Continuity Plan and Sub-Plans
CCTV System Corporate Practice
Data Breach Policy (to be adopted)
Data Breach Response Plan dated 21 December 2022
Data Breach Policy (Information and Privacy Commission NSW)
Data Sharing (Government Sector) Act 2015
Disclosure of Interests Returns Corporate Practice
General Data Protection Regulation ((EU) 2016/679)
Health Records and Information Privacy Act 2002

IT and Cyber Security Policy
Privacy Code of Practice for Local Government (June 2000)
Privacy Act 1988 (Cth)
Privacy and Personal Information Protection Act 1998
Privacy and Personal Information Protection Regulation 2019
Privacy Guidelines for Mosman Council Staff
Privacy self-assessment tool issued by Privacy and Information Commission

Review

This policy will be reviewed every four years unless otherwise directed by Council or the Executive Team.

Contact

Enquiries should be directed to the Council's Privacy Contact Officer (Manager Governance) on 9978 4000 or alternatively, for assistance in understanding the processes under the PPIPA and HRIPA, contact the Office of the Privacy Commissioner NSW.

Amendments

Date	Amendment	Reference
25 August 2000	Adopted	PF/205
6 June 2005	Various amendments including introduction of *Health Records and Information Privacy Act 2002* (HRIP Act)	CS/49
6 September 2011	Re-written to contemporise and ensure consistency with related legislation	CS/44
20 August 2012	Updated to incorporate the changes recommended by the Office of the Privacy Commissioner – 10 October 2011	DW doc. No. 2786597
9 April 2013	Adoption of Model Privacy Management Plan for Local Government as amended (DLG Circular 13-03)	CS/29
6 March 2018	Review	CS/12
1 August 2023	Review and address MNDB Scheme	CS/22
7 May 2024	Review and address outstanding Internal Audit Report recommendations	CS/12

Appendices

Appendix 1: Statutory Declaration for Access under Section 57 of the Privacy and Personal Information Protection Act 1998 to a Public Register Held by Council

Statutory Declaration
Oaths Act, 1900, Ninth Schedule

I, the undersigned (1) ..... (1) insert full name

of (2) ..... (2) insert address

in the State of New South Wales, do solemnly and sincerely declare that:

I am (3) ..... (3) insert relationship, if any, to person inquired about

I seek to know whether (4) ..... (4) insert name

is on the public register of (5) ..... (5) Applicant to describe the relevant public public register

The purpose for which I seek this information is (6) (6) insert purpose for seeking information

.....

The purpose for which the information is required is to (7) (7) insert purpose

.....

And I make this solemn declaration conscientiously believing the same to be true and by virtue of the Oats Act 1994.

.....
Signature of Applicant

Declared at: .....

in the said State this ..... day of ..... 20 .....

before me. .....
Signature of Justice of the Peace/Solicitor

.....
Name of Justice of the Peace/Solicitor to be printed

Appendix 2: Privacy Notification Form - Section 10 (Pre – Collection)

(Addressed to the person from whom information is about to be collected or has been collected.)

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

The intended recipients of the personal information are:

- officers within the Council;
- data service providers engaged by the Council from time to time;
- any other agent of the Council; and
- _____ (INSERT NAME OF OTHER INTENDED RECIPIENTS)

The supply of information by you is: ❒ Voluntary ❒ Not voluntary

If you cannot provide, or do not wish to provide, the information sought, the Council

❒ maybe unable to process your application.
❒ will be unable to process your application.

Council is collecting this personal information from you in order to:

_____

You may make application for access or amendment to information held by Council.

You may also make a request that Council suppress your personal information from a public register. Council will consider any such application in accordance with the PPIPA.

Council is to be regarded as the agency that holds the information. However, if it ***is not*** Council who holds or controls the information, please state below who does:

_____
(INSERT NAME OF AGENCY WHO HOLDS OR CONTROLS THE INFORMATION)

Enquiries concerning this matter can be addressed to: _____

_____

Signature _____

Name to be printed _____

Date signed / /

Appendix 3: Privacy Notification Form - Section 10 (Post – Collection)

(Addressed to the person from whom information has been collected.)

The personal information that Council has collected from you is personal information for the purposes of the Privacy and Personal Information Protection Act 1998 (PPIPA).

The intended recipients of the personal information are:

- officers within the Council;
- data service providers engaged by the Council from time to time;
- any other agent of the Council; and
- _____ (INSERT NAME OF OTHER INTENDED RECIPIENTS)

The supply of information by you is: ❒ Voluntary ❒ Not voluntary

If you cannot provide, or do not wish to provide, the information sought, the Council may: _____

Council has collected this personal information from you in order to:

_____

You may make application for access or amendment to information held by Council.

You may also make a request that Council suppress your personal information from a public register. Council will consider any such application in accordance with the PPIPA.

Council is to be regarded as the agency that holds the information. However, if it ***is not*** Council who holds or controls the information, please state below who does:

_____

(INSERT NAME OF AGENCY WHO HOLDS OR CONTROLS THE INFORMATION)

Enquiries concerning this matter can be addressed to:

_____

Signature _____

Name to be printed _____

Date signed / /

Appendix 4: Application Under Section 13 of the Privacy and Personal Information Protection Act 1998: To Determine Whether Council Holds Personal Information About A Person.

Personal information held by the Council

I, (1) _____

of (2) _____

Hereby request the General Manager of (3) _____

provide the following:

(1) insert full name

(2) insert address

(3) insert name of Council

- Does the Council hold personal information about me? ❒ Yes ❒ No
- If so, what is the nature of that information? _____
- What is the main purpose for holding the information? _____
- Am I entitled to access the information? ❒ Yes ❒ No

My address for response to this application is:

_____

_____ State: _____ Post Code: _____

Note to applicants

Council **will not** record your address or any other contact details that you provide for any other purpose other than to respond to your application.

As an applicant, you have a right of access to personal information concerning yourself that is held by the Council under section 14 of the Privacy and Personal Information Protection Act 1998 (PPIPA). There is a separate application form to gain access.

The Council may refuse to process this application in part or in whole if:

- there is an exemption to section 13 of the PPIPA; or
- a Code of Practice may restrict the operation of section 14.

Enquiries concerning this matter can be addressed to:

Appendix 5: Application Under Section 14 of the Privacy and Personal Information Protection Act 1998: For Access To Applicant's Personal Information

Personal information held by the Council

I, [1] _____

of [2] _____

Hereby request that the[3] _____

_____

Provide me with:

(1) insert full name

(2) insert address

(3) insert name of Council

- ❒ (a) access to all personal information held concerning myself; or
- ❒ (b) access to the following personal information only **(LIST INFORMATION REQUIRED BELOW):**

_____

_____

My address for response to this application is:

_____

_____ State: _____ Post Code: _____

Note to applicants

As an applicant, you have a right of access to personal information concerning yourself that is held by the Council under section 14 of the Privacy and Personal Information Protection Act 1998 (PPIPA).

You are entitled to have access without excessive delay or cost.

Council may refuse to process your application in part, or in whole, if:

- the correct amount of fees has not been paid;
- there is an exemption to section 14 of the PPIPA; or
- a Code of Practice may restrict disclosure.

Enquiries concerning this matter can be addressed to:

_____

_____

Appendix 6: Application Under Section 15 of the Privacy and Personal Information Protection Act 1998: For Alteration of Applicant's Personal Information

Personal information held by the Council

I, (1) _____

of (2) _____

Hereby request that the(3) _____

_____

(1) insert full name

(2) insert address

(3) insert name of Council

alter personal information regarding myself in the following manner:

- I propose the following changes: _____

_____

- The reasons for the changes are as follows: _____

_____

- The documentary bases for those changes is as shown on the attached documents

_____

_____

Note to Applicants :
You have a right to request appropriate amendments are made (whether by way of corrections, deletions or additions) to ensure that the personal information held by the Council:

(a) is accurate, and
(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up-to-date, complete and not misleading.

If Council is not prepared to amend the personal information in accordance with a request by you, Council must take such steps as are reasonable to attach to the information in such a manner as is capable of being read with the information, any statement provided by you.

If your personal information is amended, you are entitled under the Privacy and Personal Information Protection Act 1998 (PPIPA), if it is reasonably practicable, to the have recipients of that information notified of the amendments made by Council.

Council may refuse to process your application in part, or in whole, if:

- there is an exemption to section 15 of the PPIPA; or
- a Code of Practice may restrict alteration.

Enquiries concerning this matter can be addressed to: _____

_____

Appendix 7: Decision Rule for Application to Access Personal Information