



# **PRIVACY MANAGEMENT PLAN**

Sutherland Shire Council

## Document review and approval

This document has been approved by

	Name	Minute No	Date approved
1	<i>Finance, Resources &amp; Management Committee FIN056-01</i>	242	28/08/2000
2	<i>Finance &amp; Management Committee FIN161-10</i>	727	10/05/2010
3	<i>Finance &amp; Management Committee FIN172-11</i>	751	16/05/2011
4	<i>Finance &amp; Management Committee FIN127-13</i>	784	06/05/2013

## Revision history

Version	Author	Date	Revision
1	<i>Director Corporate Services</i>	<i>16 August, 2000</i>	<i>Original Version</i>
2	<i>Governance Manager</i>	<i>22 April, 2010</i>	<i>Plan updated to reflect the introduction of the Government Information (Public Access) Act</i>
3	<i>Governance Manager</i>	<i>8 May, 2012</i>	<i>Plan updated to cover new Privacy areas - Information collected from websites, including Council's website, about individuals; • Disclosure of Council data to companies that provide services on behalf of Council; • Use of private information on Council's Volunteer Register.</i>
3	<i>Governance Manager</i>	<i>7 May, 2013</i>	<i>Plan updated to adopt the Revised Model Privacy Management Plan for Local Government as Council's Privacy Management Plan, with the inclusion of existing extra detailed examples of how Council will handle specific types of private information and health records and also a more detailed explanation of supporting council policies and procedures, that were contained in the previous Privacy Management Plan.</i>

# TABLE OF CONTENTS

- Privacy Management Plan ..... 1**
- Preface ..... 4**
- Part 1 – Introduction ..... 5**
  - 1.1 What is “personal information”? ..... 6
  - 1.2 What is not “personal information” ..... 6
  - 1.3 Application of this Plan ..... 7
  - 1.4 Personal Information held by Council ..... 7
  - 1.5 Applications for suppression in relation to general information (not public registers)..... 7
  - 1.6 Caution as to unsolicited information..... 8
- Part 2 – Public Registers ..... 9**
  - 2.1 Public registers, the PPIPA and the HRIPA..... 10
  - 2.2 Effect on section 6 of the GIPA Act ..... 10
  - 2.3 Where some information in the public register has been published ..... 11
  - 2.4 Disclosure of personal information contained in the public registers ..... 11
  - 2.5 Purposes of public registers ..... 11
  - 2.6 Applications for access to own records on a public register ..... 12
  - 2.7 Applications for suppression in relation to a public register ..... 12
  - 2.8 Other registers..... 13
- Part 3 – The Information Protection Principles ..... 14**
- Part 4 – Health Privacy Principles ..... 38**
- Part 5 – Implementation of the Privacy Management Plan..... 52**
  - 5.1 Training Seminars/Induction ..... 52
  - 5.2 Responsibilities of the Privacy Contact Officer ..... 52
  - 5.3 Distribution of information to the public..... 53
  - 5.4 Training and education ..... 53
- Part 6 – Internal Review ..... 54**
  - 6.1 How does the process of Internal Review operate? ..... 54
  - Privacy internal review process ..... 55
  - 6.2 What happens after an Internal Review?..... 56
- Part 7 –Relevant Policies..... 57**
- Part 8 – Other Relevant Matters ..... 59**
  - 8.1 Contracts with consultants and other private contractors ..... 59
  - 8.2 Confidentiality ..... 59
  - 8.3 Misuse of personal or health information..... 59
  - 8.4 Regular review of the collection, storage and use of personal or health information..... 59
  - 8.5 Regular review of Privacy Management Plan..... 59
  - 8.6 Further information ..... 59
- Part 9 – Appendices ..... 60**

## **PREFACE**

The *Privacy and Personal Information Protection Act 1998* (the “PPIPA”) requires all councils to prepare a Privacy Management Plan outlining their policies and practices to ensure compliance with the requirements of that Act and the *Health Records and Information Privacy Act 2002* (the HRIPA).

In particular, the object of this plan is to inform:

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

## PART 1 – INTRODUCTION

The Privacy and Personal Information Protection Act 1998 (“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 Privacy Management Plan (the “Plan”) to deal with:

- the devising of policies and practices to ensure compliance by the Council with the requirements of the PPIPA and the Health Records and Information Privacy Act 2002 (“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 (“the Code”) 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* (the “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 Application of this Plan**

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

- Councillors;
- Council employees;
- Consultants and contractors of the Council;
- Council owned businesses; and
- 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.

### **1.4 Personal Information held by Council**

The Council holds personal information concerning Councillors, such as:

- personal contact information;
- complaints and disciplinary matters;
- pecuniary interest returns; and
- entitlements to fees, expenses and facilities.

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

- rates records; and
- DA applications and objections; and
- various types of health information (see page 34 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; and
- health information (such medical certificates and workers compensation claims).

### **1.5 Applications for suppression in relation to general information (not public registers).**

Under section 739 of the Local Government Act 1993 (“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.

## **1.6 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.

## PART 2 – 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 under the LGA: \*\*\*

- Section 53 - Land Register
- Section 113 - Records of Approvals;
- Section 449 -450A - Register of Pecuniary Interests;
- Section 602 - Rates Record.

\*\*\*Note – this is purely indicative. Council may, by virtue of its own practice, hold other Public Registers, to which the PPIPA applies.

Council holds the following public registers under the Environmental Planning and Assessment Act:

- Section 100 – Register of consents and approvals
- Section 149G – Record of building certificates

Council holds the following public register under the Protection of the Environment (Operations) Act:

- Section 308 – Public register of licences held

Council holds the following public register under the Impounding Act 1993:

- Section 30 & 31 – Record of impounding

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.

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; **and**
  - (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 100 of the Environmental Planning and Assessment Act 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 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**

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 450A - 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**

Section 100 – 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 149G – 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**

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 Impounding Act**

Section 30 & 31 – Record of impounding – The primary purpose is to identify any impounding action 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.

## **PART 3 – THE INFORMATION PROTECTION PRINCIPLES**

### **What are the Information Protection Principles?**

The PPIP Act contains 12 principles relating to the collection, security, access, alteration, use and disclosure of personal information. These principles are known as Information Protection Principles (IPPs) and are in Part 2 Division 1, s 8 – 19 of the PPIP Act.

The PPIP Act also contains a number of exemptions to these IPPs. The effect of these exemptions is that in certain circumstances Council is not required to act in accordance with the IPPs.

The IPPs are also subject to codes of practice. These codes identify areas where an agency may depart from the IPPs. The applicable code for Council is the Privacy Code of Practice for Local Government ('the code'). A copy of the code is attached to this plan as Appendix "5". This code was developed to ensure that Local Government is able to fulfil its statutory duties and functions in a manner which complies with the PPIP Act.

This section of the plan includes:

- A description of each IPP and a discussion of Council's policy in relation to the particular IPP.
- The effect of any exemption under the PPIP Act or modification permitted under the code, where applicable.
- Other relevant matters in relation to the IPP.

### **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, and*
  - (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 1989
- Companion Animals Act 1998\*\*
- Conveyancing Act 1919

- Environmental Planning and Assessment Act 1979
- Fire Brigades Act 1989
- Fluoridation of Public Water Supplies Act 1957
- Food Act 1989
- Impounding Act 1993
- Library Act 1939
- Protection of the Environment Operations Act 1997
- Public Health Act 1991
- Recreation Vehicles Act 1983
- Roads Act 1993
- Rural Fires Act 1997
- State Emergency Service Act 1989
- Strata Schemes (Freehold Development ) Act 1973
- Strata Schemes (Leasehold Development ) Act 1986;
- Swimming Pools Act 1992
- Public Health Act 1991

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 Protection Act 1979;
- Environmental Offences and Penalties Act 1989;
- Government Information (Public Access) Act 2009;
- Heritage Act 1977;
- State Emergency and Rescue Management Act 1989;
- Unclaimed Money Act 1995;
- Unhealthy Building Land Act 1990.

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 Director General'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; and
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.

Although Council usually collects personal information for one main purpose, this information may be used for a variety of other purposes. For example, Council's rates records contain the names and addresses of individual property owners. This information is however also used to notify adjoining property owners of proposed developments, identify companion animal ownership and evaluate tree preservation orders.

Part of Council's functions also involve the collection and delivery of personal information to and from other public sector agencies. For example Council receives information from the Land Titles Office about changes in property ownership.

## **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.

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.

#### Information collected from websites

Council also collects personal information via its website, which may be hosted by a third party. Like many websites, we use "cookie" technology to collect additional website usage data and to improve our Services. A cookie is a small data file that is transferred to your computer's hard disk. Council may use cookies to better understand how you interact with our Services, to monitor aggregate usage by our users and web traffic routing on our Services, and to improve our Services. Most Internet browsers automatically accept cookies. If you access Council's website and do not wish this to occur you can instruct your browser, by editing its options, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit.

Council may, from time to time, collect personal information via third party websites that provide services on behalf of Council. Examples include, but are not limited to:

- On-line survey websites; Council may use online survey websites to conduct surveys and community consultation. Some surveys may collect name and contact details of respondents, usually voluntarily if a respondent wishes to be contacted about survey findings.
- On-line applications; Council may utilise on-line software applications to assist Council interact with its customers in a more efficient manner. Examples could include booking to attend Council Library Events, applying for grants etc. Whilst these applications may be accessed from Council's website, users may be re-directed to a third party website to perform such transactions. Users will always be informed that they are leaving Council's website for the transaction.

Council enters into appropriate agreements with such on-line application providers to ensure that any personal information collected through these channels is appropriately stored and dealt with. Council ensures that the provider has an appropriate Privacy policy which becomes part of any agreement. Customers who are re-directed to a third party website should make themselves familiar with the Privacy Policy of that provider.

#### Unsolicited information

Personal information received by Council which is not asked for or required is known as unsolicited information. This information is not subject to the collection principles in the PPIP Act. However Council will seek to comply with the IPPs relating to storing, using and disclosing this information.

## 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 collect 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 apply, 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.

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 take reasonable steps in the circumstances to ensure individuals are made aware of these matters.

Council's current forms and applications include a privacy statement addressing these matters. Examples of applications which will contain such statements include:

- Development application form
- Objections to development applications
- Government Information (Public Access) Act applications
- 

Similarly, Council's website contains a privacy statement which sets out the types of information that is collected when you visit our website and the purpose for which it is collected.

Before Council adopts a new form or publishes a new webpage that collects personal information, a draft will be reviewed by an appropriate officer to ensure it complies with IPP 3 and 4.

In addition to the PPIP Act, Council has adopted an Access to Information Policy. In this policy Council states that information relating to the identity of complainants is obtained by Council in confidence. If it was disclosed, the trust placed in Council would be significantly eroded. This would restrict the flow of information which is necessary for Council to effectively perform its roles. In the absence of any other factors in favour of release Council believes that these factors outweigh any public interest in releasing the information.

Council will perform a public interest test on each individual access application to determine if the details of complainants will be released to the applicant. This public interest test will be performed in accordance with s14 of the GIPA Act.

## 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, 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.*

#### **What does unreasonably intrude into a person's personal affairs mean?**

Information should be relevant to the purpose for which it was collected and must not be excessive. For example, a childcare attendee, who has had surgery and needs to recuperate, should present a medical certificate limited to stating the impact of the procedure on his/her ability to attend the service. The Council does not necessarily need to know the nature of the procedure.

#### **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**

To ensure information is held securely:

- Council will comply with the requirements of the State Records Act which covers the safe custody, preservation, accuracy, maintenance and disposal of state records.

Council also has in place:

- A Computer Resource Usage Policy which sets out the requirements in relation to IT security. These include the use of IDs, logins and passwords.
- A use, storage and retrieval of digital images policy
- 

Council's code of conduct also sets out the obligations that exist in relation to dealing with personal information. This includes a definition of what personal information is and the relevant legislation and policies that need to be complied with.

Council, to ensure efficiency, often utilises the services of other companies to assist Council in its functions, as a result of this it is necessary for Council to give information to these companies to allow the provision of a service to Council. In such situations everything reasonable will be done within Council's powers to prevent unauthorised use or disclosure, including entering into appropriate agreements to ensure that any personal information provided to these companies is appropriately stored and dealt with. Council ensures that the provider has an appropriate Privacy policy which becomes part of any agreement.

Examples of such situations include, but are not limited to:

- Bank account details of individuals wishing to pay their rates, child care fees, leisure centre memberships etc by Direct Debit are uploaded to Council's Bank to facilitate collection of monies.
- Creditor Payments and Payroll information are uploaded to Council's Bank to facilitate EFT payments

- Name and address of individuals may be provided to a private Mailing House provider to facilitate large Council mail outs such as Council rates notices.
- Contact details of participants in Council's "Your Shire, Your Say Residents' Panel" are provided to an external email marketing company to allow efficient and effective communication between Council and the participants of the Panel. All participants in the Panel have elected to participate and receive communications from Council.

NB: Banks are bound by the provisions of the Commonwealth Privacy Act 1988

#### 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 *Government Information (Public Access) Act 2009* ("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.

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

Council will ensure that individuals are provided access to personal information held by Council within 20 working days. Requests for access should be made in writing and addressed to the General Manager. The appropriate application form for requesting access to personal information is attached as "Appendix 2" to this plan.

If employees of Council seek access to records held about them, such requests need to be directed to the manager of personnel.

The right to access personal information under the PPIP Act does not extend to information which is held about other people. Applications will need to be made under the GIPA Act if:

1. An individual's personal information is in documents which also have information about Others
2. Access is sought for information about someone else.

#### Staff records

According to longstanding Council practice staff have a right of access to certain records about themselves without needing to apply under the GIPA Act or the privacy legislation. Staff may access their personal staff file (s11 file) by making a request directly to the Manager – Personnel.

#### 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 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 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**

Council welcomes proposed amendments or changes to the personal information it holds. This will ensure that all information is current, accurate, complete and relevant for the purpose for which it was collected.

Changes to personal information will require appropriate supporting documentation. The amount of documentation required will depend on how substantive the proposed amendments are. No charges are required in relation to amendments under IPP 8. The appropriate application form for requesting the alteration of personal information is attached as "Appendix 3" to this plan.

Where information is requested to be amended, the individual to whom the information relates, must make a request by way of statutory declaration. That request should be accompanied by appropriate evidence as to the cogency of the making of the amendment, sufficient to satisfy Council that the proposed amendment is factually correct and appropriate. Council may require further documentary evidence to support certain amendments.

If Council refuses to make the requested amendments, Council may attach a notation to

the information if this is requested by the individual.

If personal information is amended in accordance with IPP 8, Council will seek to notify the recipients of the information of any amendments made. This will be done as soon as possible and where it is reasonably practicable.

### 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 section 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 s.15.

### 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**

Before Council uses or discloses personal information, Council will take reasonable steps in the circumstances to ensure that the information is relevant, accurate, up to date, complete and not misleading having regard to the purpose for which the information is to be used.

These steps will depend on the age of the information, its likelihood for change and the particular function for which the information was collected. For example, information such as employee records may warrant greater checks to ensure that it is accurate and current before it is used.

### **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**

As was discussed previously in relation to IPP 1, information collected by Council may be used for a variety of purposes as part of its proper functions.

As detailed above, Council can use personal information for a purpose other than which it was collected for, if the individual has consented to such use. An example of such allowable use is Council's Volunteer Register. Council has compiled a volunteer register listing the names, contact details and areas of interest of all members of the public who volunteer to participate in Council organised activities such as bushcare, community events or Council Sub-Committees. This register is established to allow Council to tap into this energy and invite volunteers in one council activity to volunteer in other council activities. Volunteers may decline council's offer to receive information about other activities or volunteering opportunities in council if they do not want to receive such correspondence. Volunteers can choose not to be included on the register at the time of first registering or at any time by notifying Council in writing.

Council can also use personal information for a purpose other than which it was collected

for, if the other purpose it is being used for is directly related to the purpose for which it was collected. An example of such allowable use of personal information is when Council uploads childcare enrolment and payments received information to the Department Of Education & Workplace Relations so that Council can receive Child Care Benefit payments on behalf of families, to reduce their out of pocket payments.

#### 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.

#### 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 Department 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**

##### **Effect of other legislation**

Council's obligations under the GIPA Act are not affected by privacy legislation. However the GIPA Act contains limitations on access to documents in the form of public interest considerations against disclosure. These include information about personal affairs, documents containing confidential information and legal advice.

The Companion Animals Act also limits the disclosure of certain information. Under s89 of the Act it is an offence to disclose information obtained in the course of Council exercising its responsibilities under the Act. This includes information relating to the identification of companion animals and their owners and information gathered by authorised officers in the course of their enforcement functions.

#### Subpoenas and similar court orders for documents

The personal information held by the Council is often required as evidence in court and tribunal proceedings. These may be matters which do not include the Council, or litigation to which the Council is joined as a party. For all matters, the Proper Officer to be named in subpoenas and other orders is the General Manager.

All subpoenas and similar court orders are to be directed to the Council's Administration Unit. Individual departments or officers must not accept or deal with subpoenas or other orders except as directed by the General Manager.

The Council's Manager Legal Services or Public Officer will deal with any subpoenas, discovery orders or similar instruments related to legal proceedings involving the Council. No other officer is permitted to disclose Council records in relation to legal proceedings.

#### Requests from police and law enforcement agencies

Requests for information from the police must never be accepted over the telephone. Members of staff receiving requests for personal information from law enforcement agencies must direct such requests to the Administration Unit. The decision regarding disclosure of personal information will be made by Council's Privacy Officer, who may seek advice from the Manager – Legal Services. This procedure does not apply in cases where there is an imminent threat to life or safety, however even then reasonable attempts should be made to discuss the matter with the Privacy Officer or Manager – Legal Services.

#### Tax file numbers

The collection, use and disclosure of Tax file numbers within the Council is controlled by the Commonwealth Privacy Act 1988. The Commonwealth Privacy Commissioner has issued extensive, legally binding Tax file number guidelines (which are available at <http://www.privacy.gov.au>). The Council must ensure that tax file numbers are protected against loss, unauthorised access, use, modification, disclosure or other misuse.

#### 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 s.3 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 Division 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**

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.

Section 23(7) of the PPIPA permits non-compliance with Information Protection Principle 12 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) of the PPIPA permits non-compliance with Information Protection Principle 12 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 12 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(2) permits non-compliance with Information Protection Principle 12 where, in the case of health information, the consent of the person cannot reasonably be obtained and the disclosure is made by an authorised person to another authorised person. “Authorised person” means a medical practitioner, health worker, or other official or employee providing health or community services who is employed or engaged by a public sector agency.

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 Division 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.

## PART 4 – 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 *a/so* 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 council 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.

## **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.*

## **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.*

## **Health Privacy Principle 3**

### ***Collection to be from the 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.*

## **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 the 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 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 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).

## **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).

Additionally Council will ensure that any medical reports concerning staff members provided to Council, will be stored on a separate staff file contained under lock and key within the office of the Manager Personnel and will not remain on the general staff file .

## **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*
    - (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).*

## **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 Government Information (Public Access) Act 2009 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).*

## **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 day, 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 information 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 *Privacy and Personal Information Protection Act 1998*.

- (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*).*

## **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 and 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).

## **Health Privacy Principle 10**

- (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.

(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*

(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 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 a 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.*

**(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).

### Health Privacy Principle 11

(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.

(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*

(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 a 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.*
- (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).

## **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).

## **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).

## **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.

#### **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).

## **PART 5 – 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, and members of council committees 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.

### **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.

The role of Council's Privacy Contact Officer is to:

- receive advice and updated information from Privacy NSW about the implementation of the Privacy and Personal Information Protection Act 1998 and the Health Records Information Protection Act 2002
- act as a first point of contact with Privacy NSW for all matters related to privacy and personal information
- act as a focal point within their organisation for all matters related to privacy and personal information
- act as a first point of contact for members of the public for all matters related to privacy and personal information.
- disseminate information on privacy issues within the organisation
- co-ordinate the implementation of the privacy legislation in their organisation, including drawing up and reviewing Privacy Management Plans
- provide privacy training for staff about whether information is "personal information" or "health information" as defined in the legislation
- ensure that all complaints about privacy breaches and internal reviews are dealt with in the proper manner
- 

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

- (i) Whether the personal or health 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 health 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". 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.

### **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.

### **5.4 Training and education**

Council's Privacy Contact Officer/GIPA Officer is available to provide staff with advice if they have questions about privacy matters.

New employees will be given copies of this plan at induction and made aware of the IPPs and how they apply to Council's day to day functions.

All staff will be given information setting out Council's code of conduct. This code sets out the main requirements in relation to personal information. Staff will also be required to familiarise themselves with the full code of conduct available on our website.

This policy and all the others referred to in this plan are available on Council's website so council employees and the public have easy access to them.

If required, staff will be sent to external courses to provide additional information about the PPIP Act and recent decisions relating to GIPA and Privacy issues.

Council also regularly has employees attending the GIPA – Coordinators and Privacy Network meetings.

Council's annual report will include information outlining the actions taken by Council in complying with the PPIP Act and statistical information relating to any reviews we have undertaken.

## **PART 6 – 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 a council 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. Once your application is received by Council, a reviewing officer will be appointed to conduct the internal review. This officer will be a suitably qualified employee of Council who is/was not substantially involved in any matter relating to the complaint. The reviewing officer must complete their review within 60 days and ensure that the complainant is notified of the outcome of the review within 14 days of determination.

NSW Privacy legislation does not specify how a review is to be conducted, but does require that the person dealing with the application consider any relevant material submitted by:

- the applicant;
- the Privacy Commissioner.

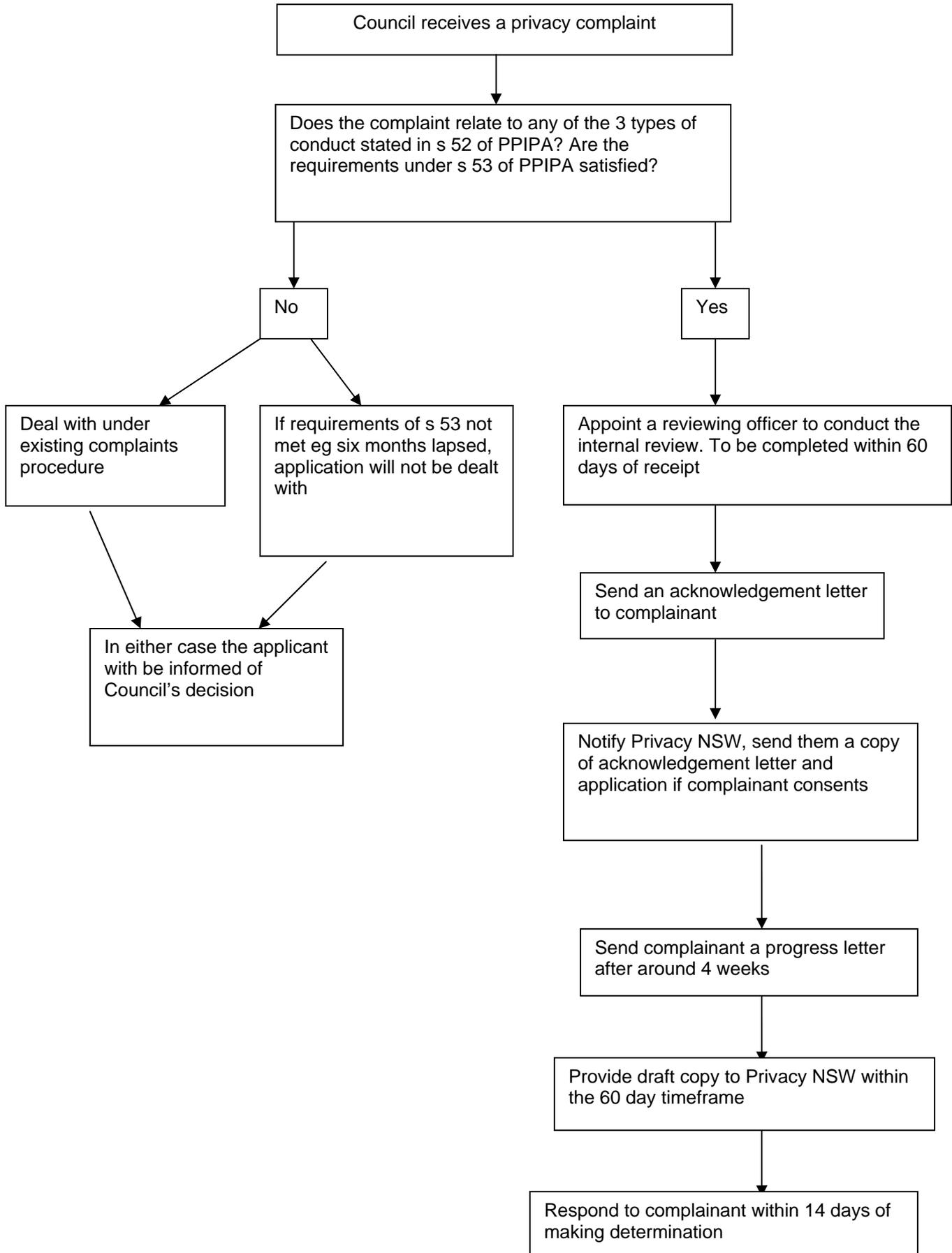
There is a checklist which provides a model of the internal review process available at the website of NSW Privacy at [http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_publications](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_publications)

A copy of the checklist is also attached as "Appendix 4" to this plan.

Council follows this checklist when processing internal privacy review applications and accordingly, before a determination is made, Council will undertake the following actions:

1. Send the complainant an acknowledgment letter setting out who the officer undertaking the review is, the date for completion, and any other relevant information relating to the review.
2. Notify Privacy NSW of the complaint and if the complainant consents, send them a copy of the application. A copy of the acknowledgment letter will also be provided to them. In addition, the NSW Privacy Commissioner is entitled to make submissions to Council in relation to the application.
3. Send the complainant a progress letter approximately four weeks after the acknowledgment letter. This letter will contain details of how the review is progressing, when it will be completed, and a reminder of the rights of review to the Tribunal if the review is not completed within the 60 day timeframe.
4. Provide a draft copy of the preliminary determination to Privacy NSW for their comment and response before sending the determination to the complainant.
5. A summary of the findings of the review must be provided to the Privacy Commissioner within 14 days of its completion

## Privacy internal review process



### Conduct following an internal review

Following the completion of the review, Council may undertake any one or more of the following:

- Take no further action in relation to the matter
- Make a formal apology to the applicant
- Take appropriate remedial action
- Provide undertakings that the conduct will not occur again.
- Implement administrative measures to ensure that the conduct does not occur again.

Council will communicate in its determination letter to the complainant the actions it will undertake following completion of the internal review.

### **6.2 What happens after an Internal Review?**

If a person is still dissatisfied after an internal review they may appeal to the Administrative Decisions Tribunal ('ADT'). The ADT hears matters afresh and imposes its own decisions. The Tribunal can decide not to take any action or make any number of the orders set out in s 55(2) of the PPIP Act. These include damages not exceeding \$40,000, an order requiring Council to take action to remedy any loss or damage, and any other order that the ADT thinks is appropriate.

## **PART 7 –RELEVANT POLICIES**

There are various policies and protocols that affect the handling of personal information by Sutherland Shire Council:

### Access to Information Policy

The objective of this policy is to describe Council's principles regarding public and Councillor access to information and to facilitate the processing of requests for such access under the Government Information (Public Access) Act 2009. This policy is to be read in conjunction with the Access to Information Guidelines.

### Workplace Surveillance Policy (Overt Surveillance)

Outlines the way Council will handle information obtained from workplace video surveillance, computer surveillance and tracking surveillance. This policy applies to all workplaces under the control and responsibility of Council where the surveillance may directly or indirectly monitor an employee (as defined in the Industrial Relations Act 1996), Council contractors, Councillors, persons performing voluntary work or any person authorised to undertake a Council function or activity while in the workplace.

The surveillance information will only be used/disclosed for legitimate employment/business purpose or in connection with suspected corruption, illegal activity, maladministration, misuse of Council resources and/or imminent threat of serious violence to persons or substantial damage to property, in accordance with Section 18 of the *Workplace Surveillance Act 2005*.

### Computer Resource Usage Policy

Outlines Council employees' responsibilities when using computers for email and internet, including disciplinary action. Also includes forms for permission to remove files from network and access to CD and DVD drives. The Policy prohibits staff from removing data from a Council computer resource without gaining prior approval, in accordance with the Policy.

### Policy Statement – Records

The Council's records are its corporate memory, provide evidence of actions and decisions and represent a vital asset to support daily functions and operations. They support policy formation and managerial decision-making, protect the interests of the organisation and of the Council as well as the rights of employees, clients and citizens, and help in the delivery of services in a consistent and equitable way. Records assist the Council to make good use of precedents and of organisational experience. They also support consistency, continuity, efficiency and productivity in program delivery, management and administration.

The Council is committed to meeting its responsibilities under the State Records Act 1998 and to implementing applicable and appropriate Policies, Standards and Codes of best practice in its records management processes and systems. All practices and procedures concerning records management within organisational areas of the Council must have regard to this policy and be available for audit.

All staff are required to observe the following rules associated with the records management system:

- staff are to use the authorised 'records' system to document all substantive official business;

- staff are not to maintain individual or separate files or unauthorised record keeping systems;
- no records are to be disposed of unless authorised by the Records Management Group and are covered by a disposal schedule authorised by State Records; or under relevant legislation as directed in part 3 of the Act; or through 'normal administrative practice' as defined in the Act. This applies to electronic records as well as 'hardcopy' records. Records disposal is addressed in more detail later;
- only authorised staff may create new files or modify or close existing files or record file movements on the authorised organisational records system;
- the location of every record should be accurate and up to date at all times. Staff are responsible for recording location changes when passing a file to another staff member, by notifying the responsible records person;
- no file should be removed from the records administration area without informing a records administration person so that records can be updated;
- staff should minimise the number of files kept on desks/in workstations and the length of time they are kept;
- files should not leave the premises, apart from exceptional circumstances and then only if authorised by a senior manager. If possible, a photocopy of relevant documents should be taken to meetings offsite. The records administration area should be informed when files are removed from the premises; and
- records including electronic files, email or other computer based information must not be removed from the network without the appropriate authorisation form being completed and approved.

## **PART 8 – OTHER RELEVANT MATTERS**

### **8.1 Contracts with consultants and other private contractors**

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

### **8.2 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.

### **8.3 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.

### **8.4 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.

### **8.5 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.

### **8.6 Further information**

For assistance in understanding the processes under the PPIPA and HRIPA, please contact the Council or the Office of the Privacy Commissioner NSW.

**PART 9 – APPENDICES**



# APPLICATION TO DETERMINE WHETHER COUNCIL HOLDS PERSONAL INFORMATION ABOUT A PERSON

Made under Section 14 of the Privacy and Personal Information Protection Act 1998

**Customer Request No:** \_\_\_\_\_ (office use only)

## Please read the following information carefully before proceeding with your application

Should you provide your address or any other contact details Sutherland Shire Council will not record those details 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 Council under section 14 of the Privacy and Personal Information Protection Act 1998. There is a separate application form to gain access to personal information.

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

- there is an exemption to section 13 of the Act; or
- or a Code of Practice may restrict disclosure.

## CONTACT DETAILS

You are required to supply your name and address for correspondence. Additional contact details will help us to deal with your application, and to correspond with you in the manner you prefer.

Title (e.g Mr, Mrs, Ms, Miss, Dr)

Given Name/s

Family Name

Postal address

Preferred method of contact (tick one option then fill out related field below. Please include area code where appropriate.)

Phone  Fax  Mobile  Email  Post

Phone:

Mob:

Email:

Fax:

## APPLICATION DETAILS

Applicants need to provide sufficient information to enable the correct document/s to be identified.

I hereby request that Sutherland Shire Council provide me with details of:

- the nature of the information held.
- the main purpose for which the information is held.
- whether I am entitled to access the information.

Please attach any documentary evidence that will form the basis for your application.

# APPLICATION FOR ACCESS to PERSONAL INFORMATION Appendix 2

Made under Section 14 of the Privacy and Personal Information Protection Act 1998

**Customer Request No:** \_\_\_\_\_ (office use only)

## Please read the following information carefully before proceeding with your application

As an applicant, you have a right of access to your personal information held by Sutherland Shire Council under section 14 of the Privacy and Personal Information Protection Act 1998.

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 have not been paid;
- there is an exemption to section 14 of the Act;
- or a Code of Practice may restrict disclosure.

## CONTACT DETAILS

You are required to supply your name and address for correspondence. Additional contact details will help us to deal with your application, and to correspond with you in the manner you prefer.

Title (e.g Mr, Mrs, Ms, Miss, Dr)

Given Name/s

Family Name

Postal address

Preferred method of contact (tick one option then fill out related field below. Please include area code where appropriate.)

Phone  Fax  Mobile  Email  Post

Phone:

Mob:

Email:

Fax:

## APPLICATION DETAILS

Applicants need to provide sufficient information to enable the correct document/s to be identified.

I hereby request that Sutherland Shire Council provide me with:

- access to all personal information held concerning myself; or
- access to the following personal information only, please give details below:

Please attach any documentary evidence that will form the basis for your application

## APPLICATION FOR ALTERATION of PERSONAL INFORMATION

Made under Section 15 of the Privacy and Personal Information Protection Act 1998

Appendix 3

Customer Request No: \_\_\_\_\_ (office use only)

### Please read the following information carefully before proceeding with your application

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 Sutherland Shire 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, if it is reasonably practicable, to 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 Act; or
- \* a Code of Practice may restrict alteration.

### CONTACT DETAILS

You are required to supply your name and address for correspondence. Additional contact details will help us to deal with your application, and to correspond with you in the manner you prefer.

Title (e.g Mr, Mrs, Ms, Miss, Dr)

Given Name/s

Family Name

Postal address

Preferred method of contact (tick one option then fill out related field below. Please include area code where appropriate.)

Phone  Fax  Mobile  Email  Post

Phone:

Mob:

Email:

Fax:

### APPLICATION DETAILS

Applicants need to provide sufficient information to enable the correct document/s to be identified.

I hereby request that Sutherland Shire Council alter personal information regarding myself in the following manner :  
I propose the following changes:

The reasons for the changes are as follows :

Please attach any documentary evidence that will form the basis for the proposed changes

## PRIVACY NSW – COMPLAINTS TO PUBLIC SECTOR AGENCIES

### INTERNAL REVIEW CHECKLIST FOR THE RESPONDENT AGENCY

The *Privacy and Personal Information Protection Act 1998* (the PPIP Act) and the *Health Records and Information Privacy Act 2002* (the HRIP Act) provide that public sector agencies deal with complaints by way of Internal Review. This process is the same under both Acts although you will be assessing the alleged conduct against different standards (the IPPs and the HPPs).<sup>1</sup>

A privacy complaint may come under:

- the PPIP Act, section 53,<sup>2</sup> if it relates to personal information, and the Information Protection Principles (IPPs), or
- the HRIP Act, section 21, if it relates to health information and the Health Privacy Principles (HPPs).

	<b>Steps to follow</b>	<b>Date completed</b>
	<b>Preliminary steps</b>	
1	<p>Is the complaint about a person's <b>personal information</b>?<sup>3</sup></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – You should treat their complaint as a request for Internal Review. Go to Q.2.</li> <li><input type="checkbox"/> No – Follow your agency's normal complaint handling procedures.</li> </ul>	
2	<p>Is the complaint about a person's <b>health information</b>?<sup>4</sup></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – You should treat their complaint as a request for Internal Review under the HRIP Act. This means that the HPPs and other standards under the HRIP Act will apply. Go to Q.3.</li> <li><input type="checkbox"/> No – You should treat their complaint as a request for Internal Review under the PPIP Act. This means that the IPPs and other standards under the PPIP Act will apply. Go to Q.3.</li> <li><input type="checkbox"/> Both – See the notes below.<sup>5</sup> Go to Q.3.</li> </ul>	
3	According to the complainant, when did the alleged conduct occur?	
4	<p>Is the complaint about conduct that occurred after 1 July 2000?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Go to Q.5.</li> <li><input type="checkbox"/> No – The PPIP Act does not apply. Follow your agency's normal complaint handling procedures.</li> </ul>	
5	<p>Is the complaint about health information and conduct that occurred after 1 September 2004?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – the HRIP Act covers this complaint. Go to Q.6.</li> <li><input type="checkbox"/> No – the PPIP Act covers this complaint. Go to Q.6</li> </ul>	
6	According to the complainant, when did they first <i>become aware</i> of the alleged conduct? <sup>6</sup>	
7	When was this application / privacy complaint first lodged? <sup>7</sup>	

8	<p>If more than six months lapsed between the date at Q.6 and the date at Q.7, your agency must decide whether you will accept a late application.<sup>8</sup></p> <p>Will you accept this late application?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Go to Q.9.</li> <li><input type="checkbox"/> No – Explain your reasons to the complainant, then follow your agency’s normal complaint handling procedures.</li> </ul>	
9	<p>When will 60 days elapse from the date at Q.7?</p> <p><i>After this date the complainant may go to the Administrative Decisions Tribunal (‘the Tribunal’) without waiting for the results of this review.</i></p>	
10	<p>For complaints about a person’s <b>health information</b> go to Q.11</p> <p>For complaints about a person’s <b>personal information</b>, not including health information, tick all of the following types of <b>conduct</b><sup>9</sup> that describe the complaint. Then go to Q.12.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> collection of the complainant’s personal information (IPPs 1-4)</li> <li><input type="checkbox"/> security or storage of the complainant’s personal information (IPP 5)</li> <li><input type="checkbox"/> refusal to let the complainant access or find out about their own personal information (IPPs 6-7)</li> <li><input type="checkbox"/> accuracy or relevance of the complainant’s personal information (IPPs 8-9)</li> <li><input type="checkbox"/> use of the complainant’s personal information (IPP 10)</li> <li><input type="checkbox"/> disclosure of the complainant’s personal information (IPPs 11-12, and/or the public register provisions in Part 6 of the Act)</li> <li><input type="checkbox"/> other / it’s not clear</li> </ul>	
11	<p>For complaints about a person’s <b>health information</b>, tick all of the following types of <b>conduct</b><sup>10</sup> which describe the complaint:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> collection of the complainant’s health information (HPPs 1-4)</li> <li><input type="checkbox"/> security or storage of the complainant’s health information (HPP 5)</li> <li><input type="checkbox"/> refusal to let the complainant access or find out about their own health information (HPPs 6-7)</li> <li><input type="checkbox"/> accuracy or relevance of the complainant’s health information (HPPs 8-9)</li> <li><input type="checkbox"/> use of the complainant’s health information (HPP 10)</li> <li><input type="checkbox"/> disclosure of the complainant’s health information (HPP 11)</li> <li><input type="checkbox"/> assignment of identifiers to the complainant (HPP 12)</li> <li><input type="checkbox"/> refusal to let the complainant remain anonymous when entering into a transaction with your agency (HPP 13)</li> <li><input type="checkbox"/> transfer of the complainant’s health information outside New South Wales (HPP 14)</li> <li><input type="checkbox"/> including the complainant’s health information in a health records linkage system (HPP 15)</li> <li><input type="checkbox"/> other / it’s not clear</li> </ul>	
12	<p>Appoint a reviewing officer. <i>(The reviewing officer must be someone who was not substantially involved in any matter relating to the conduct complained about. For other requirements see s.53(4) of the PPIP Act. This also applies to the HRIP Act.)</i></p> <p>Insert the reviewing officer’s name here:</p>	

13	<p>Write to the complainant, stating:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> your understanding of the conduct complained about,</li> <li><input type="checkbox"/> your understanding of the privacy principle/s at issue (either IPPs at Q.10 or HPPs at Q.11),</li> <li><input type="checkbox"/> that the agency is conducting an Internal Review under the PPIP Act or the HRIP Act, as appropriate,</li> <li><input type="checkbox"/> the name, title, and contact details of the reviewing officer,</li> <li><input type="checkbox"/> how the reviewing officer is independent of the person/s responsible for the alleged conduct,</li> <li><input type="checkbox"/> the estimated completion date for the review process,</li> <li><input type="checkbox"/> that if your review is not complete by the date at Q.9, the complainant can go to the Tribunal for an external review of the alleged conduct, and</li> <li><input type="checkbox"/> that a copy of this letter will be provided to the NSW Privacy Commissioner for their oversight role.</li> </ul>		
14	<p>Send a copy of your letter at Q.13 to the NSW Privacy Commissioner, at GPO Box 6, Sydney NSW 2001; or fax (02) 9228-8577.</p> <p>If the complainant has consented,<sup>11</sup> include a copy of the complainant's application – either the whole application or just the information provided at Q's 5-12 on the <i>Privacy Complaint: Internal Review Application Form</i>.</p>		
<b>Now you can start the review itself</b>			
15	<p><b><u>Under the PPIP Act</u></b></p> <p>You need to determine:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> whether the alleged conduct occurred,</li> <li><input type="checkbox"/> if so, whether the conduct complied with all the IPPs (and Part 6 public register provisions if applicable)<sup>12</sup>, and</li> <li><input type="checkbox"/> if the conduct did not comply with an IPP (or the public register provisions), whether the non-compliance was authorised by: <ul style="list-style-type: none"> <li><input type="checkbox"/> an exemption under the PPIP Act<sup>13</sup>,</li> <li><input type="checkbox"/> a Privacy Code of Practice<sup>14</sup>, or</li> <li><input type="checkbox"/> a s.41 Direction from the Privacy Commissioner.<sup>15</sup></li> </ul> </li> </ul>	<p><b><u>Under the HRIP Act</u></b></p> <p>You need to determine:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> whether the alleged conduct occurred,</li> <li><input type="checkbox"/> if so, whether the conduct complied with all the HPPs<sup>16</sup>, and</li> <li><input type="checkbox"/> if the conduct did not comply with an HPP, whether the non-compliance was authorised by: <ul style="list-style-type: none"> <li><input type="checkbox"/> an exemption under the HRIP Act<sup>17</sup>,</li> <li><input type="checkbox"/> a Health Privacy Code of Practice<sup>18</sup>, or</li> <li><input type="checkbox"/> a s.62 Direction from the Privacy Commissioner.<sup>19</sup></li> </ul> </li> </ul>	
16	<p>Four weeks after sending the letter at Q.13, send a progress report to the complainant and the Privacy Commissioner.<sup>20</sup> Include:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> details of progress of the review,</li> <li><input type="checkbox"/> if there are delays, an explanation of this and a revised estimated completion date for the review process, and</li> <li><input type="checkbox"/> a reminder that if the review is not complete by the date at Q.9, the complainant can go to the Tribunal for an external review of the alleged conduct.</li> </ul>		

On completion of the review		
17	<b><u>Under the PPIP Act</u></b>	<b><u>Under the HRIP Act</u></b>
	<p>Write up your findings about the facts, the law, and your interpretation of the law.</p> <p>Set out your preliminary determination about:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> whether there was sufficient evidence to establish that the alleged conduct occurred,</li> <li><input type="checkbox"/> which of the IPPs (and/or the public register provisions) you examined and why,</li> <li><input type="checkbox"/> whether the conduct complied with the IPPs/ public register provisions,</li> <li><input type="checkbox"/> if the conduct did not comply with an IPP or public register provision, whether the non-compliance was authorised by: <ul style="list-style-type: none"> <li><input type="checkbox"/> an exemption under the PPIP Act,</li> <li><input type="checkbox"/> a Privacy Code of Practice, or</li> <li><input type="checkbox"/> a s.41 Direction from the Privacy Commissioner, and</li> </ul> </li> <li><input type="checkbox"/> an appropriate action for the agency by way of response/ remedy.</li> </ul>	<p>Write up your findings about the facts, the law, and your interpretation of the law.</p> <p>Set out your preliminary determination about:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> whether there was sufficient evidence to establish that the alleged conduct occurred,</li> <li><input type="checkbox"/> which of the HPPs you examined and why,</li> <li><input type="checkbox"/> whether the conduct complied with the HPPs,</li> <li><input type="checkbox"/> if the conduct did not comply with an HPP, whether the non-compliance was authorised by: <ul style="list-style-type: none"> <li><input type="checkbox"/> an exemption under the HRIP Act,</li> <li><input type="checkbox"/> a Health Privacy Code of Practice<sup>21</sup>, or</li> <li><input type="checkbox"/> a s.62 Direction from the Privacy Commissioner<sup>22</sup>, and</li> </ul> </li> <li><input type="checkbox"/> an appropriate action for the agency by way of response/ remedy.</li> </ul>
18	Before completing the review, check whether the Privacy Commissioner wishes to make a submission. Ideally you should provide a draft copy of your preliminary determination to the Privacy Commissioner for comment.	
20	<b><u>Under the PPIP Act</u></b>	<b><u>Under the PPIP Act</u></b>
	<p>Finalise your determination of the Internal Review, by making one of the following <b>findings</b>:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred</li> <li><input type="checkbox"/> alleged conduct occurred but complied with the IPPs/ public register provisions</li> <li><input type="checkbox"/> alleged conduct occurred; did not comply with the IPPs/ public register provisions; but non-compliance was authorised by an exemption, Code or s.41 Direction</li> <li><input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the IPPs/ public register provisions; the non-compliance was not authorised ("<b>a breach</b>")</li> </ul>	<p>Finalise your determination of the Internal Review, by making one of the following <b>findings</b>:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred</li> <li><input type="checkbox"/> alleged conduct occurred but complied with the HPPs</li> <li><input type="checkbox"/> alleged conduct occurred; did not comply with the HPPs; but non-compliance was authorised by an exemption, Code or s.62 Direction</li> <li><input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised ("<b>a breach</b>")</li> </ul>
21	<p>Did the agency breach an IPP or public register provision?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Go to Q.23.</li> <li><input type="checkbox"/> No – Go to Q.22</li> </ul>	<p>Did the agency breach an HPP?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Go to Q.23.</li> <li><input type="checkbox"/> No – Go to Q.22</li> </ul>

22	<p>Even though the agency did not breach any IPP, public register provision or HPP, have you identified any need for improvement in policies, procedures, communicating with your clients, etc?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Go to Q.23.</li> <li><input type="checkbox"/> No – Go to Q.25.</li> </ul>	
23	<p>What action is proposed by the agency as a result of this review? <i>(You can have more than one.)</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> apology to complainant</li> <li><input type="checkbox"/> rectification<sup>23</sup> to complainant, eg: <ul style="list-style-type: none"> <li><input type="checkbox"/> access to their personal information or health information</li> <li><input type="checkbox"/> correction of their personal information or health information</li> <li><input type="checkbox"/> other type of rectification</li> </ul> </li> <li><input type="checkbox"/> expenses paid to complainant</li> <li><input type="checkbox"/> compensatory damages paid to complainant</li> <li><input type="checkbox"/> other remedy to complainant</li> <li><input type="checkbox"/> review of policies, practices or systems</li> <li><input type="checkbox"/> change in policies, practices or systems</li> <li><input type="checkbox"/> training (or further training) for staff</li> <li><input type="checkbox"/> other action</li> <li><input type="checkbox"/> no action</li> </ul>	
24	<p>Is the proposed action likely to match the expectations of the complainant?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes</li> <li><input type="checkbox"/> No</li> <li><input type="checkbox"/> Unsure</li> </ul>	

25	<p><b><u>Under the PPIP Act</u></b></p> <p>Notify the complainant and the Privacy Commissioner<sup>24</sup> in writing:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> that you have completed the Internal Review,</li> <li><input type="checkbox"/> what your <b>findings</b> are, i.e. which one of the following: <ul style="list-style-type: none"> <li><input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred</li> <li><input type="checkbox"/> alleged conduct occurred but complied with the IPPs/ public register provisions</li> <li><input type="checkbox"/> alleged conduct occurred; did not comply with the IPPs/ public register provisions; but non-compliance authorised by an exemption, Code or s.41 Direction</li> <li><input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the IPPs/ public register provisions; the non-compliance was not authorised ("<b>a breach</b>")</li> </ul> </li> <li><input type="checkbox"/> what the <b>reasons</b> for your findings are,</li> <li><input type="checkbox"/> a plain English explanation of the <b>law</b> behind your findings, including quoting in full the relevant legislative provisions you are talking about,</li> <li><input type="checkbox"/> what action/s you are going to take as a result,</li> <li><input type="checkbox"/> that the complainant has the right to apply to the Tribunal for a review of the conduct complained about, and</li> <li><input type="checkbox"/> the contact details for the Tribunal.</li> </ul>	<p><b><u>Under the HRIP Act</u></b></p> <p>Notify the complainant and the Privacy Commissioner<sup>25</sup> in writing:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> that you have completed the Internal Review,</li> <li><input type="checkbox"/> what your <b>findings</b> are, i.e. which one of the following: <ul style="list-style-type: none"> <li><input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred</li> <li><input type="checkbox"/> alleged conduct occurred but complied with the HPPs</li> <li><input type="checkbox"/> alleged conduct occurred; did not comply with the HPPs; but non-compliance authorised by an exemption, Code, or s.62 Direction</li> <li><input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised ("<b>a breach</b>")</li> </ul> </li> <li><input type="checkbox"/> what the <b>reasons</b> for your findings are,</li> <li><input type="checkbox"/> a plain English explanation of the <b>law</b> behind your findings, including quoting in full the relevant legislative provisions you are talking about,</li> <li><input type="checkbox"/> what action/s you are going to take as a result,</li> <li><input type="checkbox"/> that the complainant has the right to apply to the Tribunal for a review of the conduct complained about, and</li> <li><input type="checkbox"/> the contact details for the Tribunal.</li> </ul>	
26	Keep a record of this review for your annual reporting requirements. <sup>26</sup>		

## NOTES

<sup>1</sup> The 12 information protection principles (IPPs) in the PPIP Act are legal obligations the manner in which NSW government agencies (including statutory bodies and local councils) must handle personal information. The 12 IPPs cover the collection, storage, use and disclosure of personal information as well as access and correction rights.

The 15 health privacy principles (HPPs) in the HRIP Act are legal obligations describing the manner in which NSW public sector agencies and private sector organisations and individuals, such as businesses, private hospitals, GPs, gyms and so on must handle health information. The 15 HPPs prescribe what an organisation must do when it collects, stores, uses and discloses health information. The HPPs also cover access and correction rights.

<sup>2</sup> S.53(1): a person (the applicant) who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct. The requirements for an application for Internal Review are as follows:

s. 53(3): An application for such a review must:

- (a) be in writing, and
- (b) be addressed to the public sector agency concerned, and
- (c) specify an address in Australia to which a notice under subsection (8) may be sent, and
- (d) be lodged at an office of the public sector agency within 6 months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct the subject of the

---

application, and

(e) comply with such other requirements as may be prescribed by the regulations (*there are no additional requirements prescribed at this time.*)

<sup>3</sup> “Personal information” is defined at s.4 of the PPIP Act as “information or an opinion ... about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion”. There are some exemptions to the definition (eg. for “information or an opinion about an individual’s suitability for appointment or employment as a public sector official”) so check s.4 in full. However if you are thinking of relying on one of these exemptions, especially s.4(3)(b) or s.4(3)(j), please first seek advice from Privacy NSW as to the extent to which the exemption applies.

<sup>4</sup> “Health information” is defined at s.6 of the HRIP Act as “personal information that is information or an opinion about the physical or mental health or a disability of an individual; express wishes about the future provision of health services; a health service provided or to be provided; any other personal information collected to provide or in providing a health service”. The definition also includes information having to do with organ donation and genetic information. There are some exemptions to the definition in s.5 of the HRIP Act (eg. for “information or an opinion about an individual’s suitability for appointment or employment as a public sector official”) so check the Act. However if you are thinking of relying on one of these exemptions, especially s.5 (3)(b) or s.5 (3)(m), please first seek advice from Privacy NSW as to the extent to which the exemption applies.

<sup>5</sup> If it is easy to distinguish between what is health information and what is other personal information then apply the relevant Act to each piece of information the subject of the complaint. If it is unclear which Act should apply, or it is too difficult to deal with the information in distinct parts, then in our view, it is best to take a cautious approach and apply both Acts to *all* the information the subject of the complaint.

<sup>6</sup> Note that in *Y v DET*, the ADT warned against agencies using ‘self-serving calculations’ when determining the date on which the complainant may have first become aware of the conduct complained of.

<sup>7</sup> In *Y v DET*, the ADT found that “express reference” to the PPIP Act is not essential in correspondence with agencies, especially where the context suggests that a statutory right is being invoked. Therefore the complainant need not have used the phrase ‘Internal Review’ for their privacy complaint to be considered by law to be an Internal Review application. Agencies should therefore look to the date the first written complaint about a breach of privacy was made

<sup>8</sup> Your agency should have a clear and written policy on the grounds under which you will allow a late application, including the means by which you will notify complainants about those grounds and what the complainant must prove to you. Include your policy in your Privacy Management Plan. For more on this issue see the April 2003 *PCO Newsletter*, available on our website via <http://www.lawlink.nsw.gov.au/pc.nsf/pages/generalinfo>

<sup>9</sup> ‘Conduct’ can include an action, a decision, or even inaction by your agency. For example the ‘conduct’ in this case might be a *decision* to refuse the complainant access to his or her personal information, or the *action* of disclosing his or her personal information to another person, or the *inaction* of a failure to protect the complainant’s personal information from being inappropriately accessed by someone else.

<sup>10</sup> See footnote 8 above.

<sup>11</sup> See Q.14 on the *Privacy Complaint: Internal Review Application Form*, if they have used that form. (It is not compulsory for the complainant to use any particular format, so long as their request is in writing.)

<sup>12</sup> Don’t forget to look at all the IPPs, as they can be inter-related. For example a complaint about disclosure (IPPs 11 and 12 and the public register provisions) might also raise issues about data security under IPP 5, or notification about collection at IPP 3.

<sup>13</sup> Exemptions are found in the PPIP Act at sections 4-6, 20, and 23-28.

<sup>14</sup> Privacy Codes of Practice are instruments made by the Attorney General (under the PPIP Act). Many can be found on the Privacy NSW website at: <http://www.lawlink.nsw.gov.au/pc.nsf/pages/codesmade>

<sup>15</sup> Section 41 Directions only modify the IPPs, not the public register provisions. These Directions are usually temporary so check the dates carefully, and contact Privacy NSW for earlier versions of Directions if necessary. All current s.41 Directions can be found at: <http://www.lawlink.nsw.gov.au/pc.nsf/pages/section41orders>.

---

<sup>16</sup> Don't forget to look at all the HPPs, as they can be inter-related. For example a complaint about disclosure (HPP 11) might also raise issues about data security under HPP 5, or notification about collection at HPP 4.

<sup>17</sup> Exemptions are found in the HRIP Act at sections 5, 10, 13-17, 22 and within the HPPs in Schedule 1.

<sup>18</sup> Health Privacy Codes of Practice are instruments made by the Attorney General (under the HRIP Act). No Health Privacy Codes of Practice have been made to date. To see some Privacy Codes of Practice go to the Privacy NSW website at: <http://www.lawlink.nsw.gov.au/pc.nsf/pages/codesmade>

<sup>19</sup> Section 62 Directions modify the HPPs. These Directions will usually be temporary so check the dates carefully. To date no s.62 Directions have been passed.

<sup>20</sup> You are obliged under section 54(1)(b) of the PPIP Act to keep the Privacy Commissioner notified of progress. This also applies to the HRIP Act.

<sup>21</sup> To date no Health Privacy Codes of Practice have been made.

<sup>22</sup> To date no s.62 Directions have been passed.

<sup>23</sup> 'Rectification' means putting things right, the way they should have been in the first place.

<sup>24</sup> Sections 53(8) and 54 of the PPIP Act.

<sup>25</sup> Sections 53(8) and 54 of the PPIP Act; this also applies to the HRIP Act.

<sup>26</sup> The annual report of each public sector agency must include statistical details of any Internal Review conducted: see s.33(3) of the PPIP Act; this also applies to the HRIP Act.



Department of Local Government  
Circular to Councils

Circular No: 00/44  
Date: 04/07/00  
File No: AF00/0043/02  
Contact: Anna Johnston  
(02) 9793 0892  
johnston.a@dlg.nsw.gov.au

**PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998**  
—  
**PRIVACY CODE OF PRACTICE FOR LOCAL GOVERNMENT**

The Privacy Code of Practice for Local Government has been approved by the Attorney General, and was made by Order published in the Government Gazette on 30 June 2000 (page 6035). The Code takes effect from 1 July 2000.

The Privacy Code of Practice for Local Government has the effect of modifying the application of Part 6 of the Privacy and Personal Information Protection Act 1998 (the “public register” provisions) and the application of the 12 Information Protection Principles as they apply to local government.

By virtue of s.32 of the Privacy and Personal Information Protection Act 1998, Council must comply with any Privacy Code of Practice that applies to it.

In addition to the Privacy Code of Practice for Local Government it is anticipated that an Investigative Code of Practice will also be made by the Attorney General shortly, which will impact upon council's investigative functions. Details on the expected application of the Investigative Code of Practice were provided in the Model Privacy Management Plan, forwarded to councils in circular 00/41. However such provisions cannot be relied upon until councils have been notified by Privacy NSW that the Code has actually been made.

**Garry Payne**  
**Director General**

# **PRIVACY CODE OF PRACTICE FOR LOCAL GOVERNMENT**

Under the Privacy and Personal Information  
Protection Act 1998 (NSW)

June 2000

# PRIVACY CODE OF PRACTICE

- A. The Privacy and Personal Information Protection Act 1998 (the “PPIPA”) provides for the protection of personal information, and for the protection of privacy of individuals generally.
- B. This Privacy Code of Practice (the “Code”) is made under Part 3 Division 1 of the PPIPA.
- C. The effect of this Code is to modify :
- ◆ the Information Protection Principles contained in Part 2, Division 1 of the PPIPA; and
  - ◆ the provisions of Part 6 of the PPIPA,
- as they relate to Local Government.
- D. Each council must have a Privacy Management Plan (the “Plan”). The Plan will outline processes to complement this Code.
- E. Questions of interpretation and application in particular circumstances may require legal advice and such advice should be obtained where it appears appropriate.
- F. The operative elements of this Code so far as the Information Protection Principles and Part 6 of the PPIPA are modified, are shown in Part 3 with respect to public registers and in Part 4 after the relevant Information Protection Principle and marked “Modification”.
- G. Explanatory notes contained in this guide serve no legal purpose of interpretation and are intended only for the purpose of clarification, or expansion.
- H. This Code applies to councillors, employees and customers of Council.
- I. This Code applies to that part of the information collected or held by Council that is personal information.
- J. Questions or written communications concerning the application of this Code or Council’s Privacy Management Plan should be addressed to the Council’s Privacy Contact Officer.
- K. This Code was gazetted on \_\_\_\_\_ 2000.

## **1 Interpretation**

**Code** means this Code of Practice;

**Council** refers to both “councils” and “county councils” under the Local Government Act 1993;

**Information Protection Principles** (“IPPs”) means those principles contained in Part 2 Division 1 of the PPIPA;

**Other Privacy Codes of Practice** refers to all Codes of Practice which apply to Council from time to time, and includes the Investigations Code of Practice and any Research Code of Practice developed by Privacy New South Wales and made by the Attorney General;

**Personal Information** has the same meaning as in PPIPA;

**PPIPA** means the Privacy and Personal Information Protection Act 1998 (NSW);

**Privacy Management Plan** means the Council’s Privacy Management Plan;

**Public Sector Agency** has the same meaning as in PPIPA;

**Public Sector Official** has the same meaning as in PPIPA and includes an officer of Council;

**Section** refers to a section of the PPIPA unless otherwise indicated.

## **2 Modifications to Public Registers**

A council may allow any person to:

- i. inspect a publicly available copy of a public register in council premises, and
- ii. copy a single entry or a page of the register

without requiring the person to provide a reason for accessing the register and without determining that the proposed use of the register is consistent with the purpose of the register or the Act under which the register is kept.

In particular a council should not require any person to provide a reason for inspecting the council's pecuniary interest register or any register on which the council records declarations made by councillors or designated officers under Chapter 14 Part 2 Divisions 3 or 4 of the Local Government Act.

Requests for access, copying or sale of the whole or a substantial part of a Public Register held by Council may not necessarily fit within the purpose for which a Public Register was created. Council may therefore:

- (i) disclose by way of providing access, copy or sale of the whole or a substantial part of a Public Register, provided that the names and addresses of all current and previous property owners and the names and addresses of all current and previous applicants are not disclosed; or
- (ii) disclose by way of providing access, copy or sale of the whole or a substantial part of a Public Register where Council has satisfied itself by way of statutory declaration by the person requesting the information that the information is to be used for a purpose of the Register or the Act under which the Register is kept. (In this respect, Council must first determine for itself the "purpose of the Register or the Act under which the Register is kept", but may be guided by the provisions of the model Privacy Management Plan for Local Government.)

With respect to both (i) or (ii) above, Council must also ensure that the provisions of section 12(1A) Local Government Act 1993 and section 149G of the Environmental Planning and Assessment Act 1979 are complied with, where applicable.

### **3 The Information Protection Principles**

The Council will apply the information protection principles as follows:

#### **Information protection principle 1 – section 8 of the PPIPA**

##### **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, and
  - (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.

##### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

#### **Information protection principle 2 – section 9 of PPIPA**

##### **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.

##### **Modification**

Council may 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.

##### **Explanatory Note**

Council may wish to confer a special award, prize, benefit or similar form of personal recognition to an individual. This may take the form of a citizen of the year award, the naming of a park after that individual, or other similar form of public recognition.

## **Information protection principle 3 – section 10 of the PPIPA**

### **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.

### **Modification**

Council may 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.

## **Information protection principle 4 – section 11 of the PPIPA**

### **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, 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.

### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

## **Information protection principle 5 – section 12 of the PPIPA**

### **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.

#### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

## **Information protection principle 6 – section 13 of the PPIPA**

### **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.

#### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

## **Information protection principle 7 – section 14 of the PPIPA**

### **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.

#### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

## **Information protection principle 8 – section 15 of the PPIPA**

### **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.

#### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

## **Information protection principle 9 – section 16 of the PPIPA**

### **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.

#### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

## **Information protection principle 10 – section 17 of the PPIPA**

### **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.

### **Modification**

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**

For example with respect to exemption (i) above, the Rates Record that Council holds under section 602 of the Local Government Act may also be used to:

- notify neighbours of a proposed development;
- evaluate a road opening; or
- evaluate a tree preservation order.

## **Information protection principle 11 – section 18 of the PPIPA**

### **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.

### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time, and 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.
4. A disclosure of personal information for research purposes will be allowed under a section 41 Direction made by the Privacy Commissioner (if such a direction exists) until such time as a Research Code of Practice is made by the Attorney General.

## **Information protection principle 12 – section 19 of the PPIPA**

### **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, 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.

(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 unless:

(a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, 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, within the year following the commencement of this section, to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales.

(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.

### **Modification**

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time except 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.

2. A disclosure of personal information for research purposes will be allowed under a section 41 Direction made by the Privacy Commissioner (if such a direction exists) until such time as a Research Code of Practice is made by the Attorney General.

## **4 Implementation of this Code of Practice**

The General Manager of Council is responsible for the implementation of this Code of Practice.

### **Compliance**

This Code will be made by an order published in the Government Gazette. This Code takes effect once the order making this Code is published (or such later date as may be specified in the order) and the Council to whom this Code applies must comply with its provisions.

The Council's Privacy Management Plan includes provisions to comply with the obligations imposed by the PPIPA having regard to this Code.

### **Complaints**

Complaints in respect of the protection and obligations arising under PPIPA and this Code should be addressed to the General Manager of the Council. All complaints will then be forwarded to the Privacy Contact Officer for review.

Complaints may alternatively be directed to the Privacy Commissioner.

### **Review of Code**

The Council will review this Code at regular intervals of not more than three years to ensure that it is optimising its compliance measures whereby personal information is collected, stored, used and disseminated.