



Privacy Management Plan



Wentworth LGA

Our Objectives

- 1 *Wentworth Shire is a vibrant, growing and thriving region*
- 2 *Wentworth Shire is a great place to live*
- 3 *Wentworth Shire is a community that works to enhance and protect its physical and natural environment*
- 4 *Wentworth Shire is supported by strong and ethical civil leadership with all activities conducted in an open, transparent and inclusive manner*

Our Values

HONESTY & INTEGRITY

ACCOUNTABILITY &
TRANSPARENCY

RESPECT

QUALITY & COMMITMENT



contents

Introduction	04
Purpose	04
Objective	04
What this plan covers	05
What is personal information	05
What is health information	05
What is not personal or health information	05
Scope	06
Legislative framework	06
Definitions	07
How Council collects and manages personal information and health information	08
i. How Council collects personal information	08
ii. Personal information held by Council	08
iii. Privacy and personal information protection notice	09
iv. Storage, access and accuracy of personal information	09
v. Use and disclosure of personal information	10
Unsolicited information	10
Publicly available information	10
Suppression of information available for public inspection (not held in public registers)	11
Mandatory proactive release of information under Section 6 of the GIPA Act	11

Acknowledgement of Country

We acknowledge the traditional owners of the land on which we live and work, and pay our respects to their elders past, present, and emerging.

Images in this document were sourced from Council's Image Library unless otherwise stated.

Cover image: Local growers block in Wentworth Shire.

This document was compiled by Wentworth Shire Council.

Copies of this program can be viewed online at wentworth.nsw.gov.au

© Copyright Wentworth Shire Council.

Document modified: 23 August 2023

Public registers	12
i. Council's public registers	12
ii. Disclosure of personal information contained in public registers	12
iii. Application for access to one's own records on a public register	13
iv. Suppression of information in relation to a public register	13
v. Other registers	13
How to access and amend personal information	13
Limits on accessing and amending information	14
Data breaches	14
i. How we will manage a data breach	14
ii. Mandatory notification of data breach (MNDB) scheme	15
Review rights and the complaints process	15
i. Internal review	15
ii. The role of the Privacy Commissioner in the review process	16
iii. External review by the NSW Civil and Administrative Tribunal NCAT	16
Promoting privacy	17
i. Compliance Strategy	17
ii. Communication Strategy	17
iii. Promoting the Plan to the Community	17
Privacy and other legislation	18
1. Collection of personal information for lawful purposes (IPP 1 & HPP 1)	18
2. Collection of personal information directly from the individual (IPP 2 & HPP 3)	19
Exemption(s) for IPP 2	19
3. Requirements when collecting personal information (IPP 3 & 4 and HPP 2 & 4)	20
Closed Circuit Television (CCTV)	21
Exemption(s) for IPP 3	21
Exemption(s) for HPP 4	22
4. Retention, destruction and security of personal information (IPP 5 and HPP 5)	22
Exemption(s) for HPP 5	22
5. Transparency and access (IPP 6 & 7 and HPP 6 & 7)	23
Exemption(s) for IPP 6 and IPP 7	24
Exemption(s) for HPP 6 & 7	25
6. Alteration, modification or amendment of personal information (IPP 8 and HPP 8)	25
Exemption(s) for HPP 8	25

7. Accuracy of information check before use (IPP 9 and HPP 9)	25
8. Limits on use of personal information (IPP 10 and HPP 10)	27
Exemption(s) for IPP 10	27
Exemption(s) for HPP 10	28
9. Restrictions and limits on disclosure of personal information (IPP 11 and HPP 11)	29
Exemption(s) for IPP 11	30
Exemption(s) for HPP 11	32
10. Special restrictions on disclosure of personal information (IPP 12)	32
Exemption(s) for IPP 12	32
11. Identifiers (HPP 12)	33
12. Anonymity (HPP 13)	33
13. Transborder data flows and data flow to Commonwealth Agencies (IPP 12 and HPP 14)	33
Exemption(s) for IPP 12	33
14. Authorised	34
Implementation of the plan	34
Training - Council staff (including employees, contractors, consultants and councillors)	34
Distribution of information	35
Confidentiality	35
Prevention of misuse of information	35
Penalties for misuse of personal or health information	35
Contact details	37
Appendix 1	
Statutory Declaration for access under Section 57 of the <i>Privacy and Personal Information Protection Act 1998</i> to a Public Register held by Council	39
Appendix 2	
Privacy Complaint: Internal review application form	40
Document approval	41

Introduction

This Privacy Management Plan (Plan) explains how Wentworth Shire Council (Council) manages personal and health information.

Purpose

Section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires that all NSW councils prepare, implement and periodically review a Privacy Management Plan (Plan).

The Plan must outline all policies, procedures and practices adopted by Council to ensure compliance with the PPIP Act, the *Health Records and Information Privacy Act 2002* (HRIP Act) and the *Privacy Code of Practices for Local Government 2000* (Privacy Code).

The purpose of this plan is to outline to the community and Council staff, the principles, procedures and guidelines that are followed by Council in order to achieve and maintain compliance in relation to:

- The collection, use, storage, security and destruction of personal and health information; and
- The access to, and disclosure of, personal and/or health information to a person or persons.

Objective

The Plan is intended to provide specific guidance and instructions to the community and Council staff on:

- The manner in which personal and health information is collected, stored, secured, used, accessed, disclosed and destroyed by Council;
- How members of the community may access, amend and update any personal or health information collected and stored by Council;
- The steps to be taken in the event that an individual believes that Council has breached its obligations under the PPIP Act and/or the HRIP Act in relation to that individual's personal or health information;
- The processes and procedures followed by Council in relation to any identified breaches of personal or health information;
- How Council policies and procedures are developed and implemented in accordance with relevant legislation and guidelines by the Information and Privacy Commissioners NSW;
- How Council disseminates these policies and procedures within Council and trains

employees in their use;

- The internal and external review processes and procedures in relation to the management of personal and health information; and
- Anything else Council considers relevant to the Plan in relation to privacy and the management of the personal and health information it holds.

The Plan supports and is supported by various policies and procedures Wentworth Shire Council has in place including:

- Wentworth Shire Council's Privacy Policy – outlines how Council will safeguard personal information held by Council and explains how personal information is to be dealt with including its use and disclosure. It is publicly available on Council's website;
- Wentworth Shire Council's Code of Conduct sets standards of conduct for Council officials that include the requirement to comply with Privacy legislation, the Information Privacy Principles and Health Privacy Principles and the Privacy Code of Practice for Local Government;

- Council also has operational policies that describe internal procedures to inform staff including a Records and Information Management Policy which references taking all reasonable steps to protect information Council holds, including personal information, from misuse and loss and from unauthorised access, modification or disclosure;
- Council provides updates to staff with reminders and access to information regarding our privacy obligations and share information to staff and the Community through participation in the Privacy Awareness Week activities;
- Wentworth Shire Council's Public Access to Information Held by Council (GIPA) Policy – provides an overview of the actions that are to be taken by Council in an endeavour to ensure that legitimate requests for access to information are handled promptly and that members of the public are able to access information, subject to the need to protect the privacy of others. This policy is available on Council's website.

What this plan covers

Section 33(2) of the PPIP Act sets out the requirements of this Plan. This Plan must include:

- information about Council's policies and practices to ensure compliance with the PPIP Act and the HRIP Act;
- how employees, contractors and volunteers are made aware of these policies and practices;
- the internal review procedures; and
- anything else considered relevant to the Plan in relation to privacy and the personal and health information Council holds.

Any reference to employees in this document also includes reference to contractors and volunteers.

What is personal information?

Personal information under Section 4 of the PPIP Act is defined as 'information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'. Personal information can include a person's name, address, information about a person's family life, information about a person's sexual preferences, financial information, photos, etc. This information can be on a database and does not necessarily have to be recorded in a material form.

What is health information?

Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act as 'personal information that is information or an opinion about the physical, mental health or disability of a person, express wishes about the future provision of health services, a health service provided or to be provided, or any other personal information collected to provide or in providing a health service.'

Health information can include information about a person's physical or mental health such as a psychological report, blood test or an x-ray, results from drug and alcohol tests, and information about a person's medical appointments. It can also include some personal information that is collected to provide a health service, such as a name and telephone number.

What is not personal information?

The PPIP Act specifically excludes the following information from the definition of what constitutes 'personal information' for the purposes of the Act:

- Information about an individual who has been dead more than 30 years;
- Information about an individual that is contained in a publicly available publication;
- Information about an individual that is contained in a public interest disclosure within the meaning of the Public Interest Disclosure Act 1994, or that has been collected in the course of an investigation arising out of a public interest disclosure;
- Information about a witness who is included in a witness protection program;

- Information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*;
- Information about an individual arising out of a Royal Commission or Special Commission of Inquiry;
- Information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990*;
- Information about an individual that is contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009*.
- Information or an opinion about an individual's suitability for appointment or employment as a public sector official;
- Information about an individual that is obtained under Chapter 8 (Adoption Information) of the *Adoption Act 2000*;
- Information about an individual that is of a class, or is contained in a document of a class, prescribed by section 5 of the PPIP Regulation.

Section 4A of the PPIP Act specifically excludes from the definition of 'personal information' any health information defined under section 6 (a) to (e) of the HRIP Act.

Scope

The Plan applies to all Council officials including (but not limited to):

- Councillors;
- Council employees, including all permanent or temporary full time, part time or casual staff;
- Consultants and Contractors of Council;
- Council-owned businesses;
- Council committees; and
- Volunteers.

Council will take reasonable steps to ensure that all such parties are made aware that they must comply with the PPIP Act, the HRIP Act, any other applicable Privacy Code of Practice and this plan.

Legislative Framework

The protection of personal and health information is governed by a number of NSW and Federal Acts of Parliament that Council is subject to and includes:

- *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- *Privacy and Personal Information Protection Regulation 2014* (PPIP Regs)
- *Health Records and Information Privacy Act 2002* (HRIP Act)
- *Health Records and Information Privacy Regulation 2017* (HRIP Regs)
- *Government Information (Public Access) Act 2009* (GIPA Act)
- *Government Information (Public Access) Regulation 2009* (GIPA Regs)
- *State Records Act 1998* (SR Act)
- *Privacy (Tax File Number) Rule 2015 – s 17 Privacy Act (Cth) 1998* (Privacy Tax Rule)
- *Privacy Code of Practice for Local Government 2000* (Privacy Code)
- *Public Interest Disclosure Act 1994* (PID Act)
- *Local Government Act 1993* (LG Act)
- *Guide to Making Privacy Management Plans* (IPC, December 2022)
- *Privacy Management Plans – Checklist* (IPC, September 2019)

These Acts of State and Federal Parliament contain specific provisions that describe the manner in which personal and health information is to be handled by Council.

DEFINITIONS

Collection (of personal information) the way in which Council acquires personal or health information, which can include a written or online form, a verbal conversation, a voice recording, email, letter, photograph or video.

Council Staff (also known as Public Sector Officials or Council Officials) includes Councillors; Council employees including all permanent or temporary full time, part time and casual staff, consultants, volunteers; contractors; administrators, delegates and internal or external members of Council committees.

Disclosure (of personal or health information) occurs when Council makes known to an individual or entity personal or health information not previously known to them.

Express consent means consent that is clearly and unmistakably communicated and is given with precise knowledge of the kind (and possibly the exact contents) of information to which the consent relates.

Impracticable means impossible in practice. (For example, it is impracticable to obtain consent from an individual if they have died, the age/volume of information is such that it would be impossible to track them down, there is no current contact details or there is insufficient information to obtain current contact details).

Law enforcement means activities or actions undertaken in response to any known or suspected breach of criminal law and/or enforcement of that law under any criminal law, Act or statute.

Privacy principles means the Information Protection Principles set out in Division 1 of Part 2 of the PPIP Act and Health Privacy Principles set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Within these principles lawful exemptions are provided.

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).

Privacy obligations means the privacy principles and any exemptions to those principles that apply to Council as a local government agency.

Transborder data flow means the movement of information from one jurisdiction to another. Borders may be local, state, federal or international and include geographical and political borders.

Transborder consent means express consent (as defined above) that includes the following knowledge:

- That the information will likely be sent to a person(s) or body(s) outside of NSW jurisdiction; and
- That the person(s) or body(s) might not be bound by privacy principles that could be enforced by the individual.

How Council collects and manages personal and health information

The LG Act confers both regulatory and service functions to Council that may deal with Personal Information, some of which may include:

- Providing for development in the local area;
- Providing local services and facilities that benefit ratepayers, residents and visitors;
- Protecting the health, wellbeing and interests of the local community;
- Representing and promoting the interests of the ratepayers and residents;
- Establishing and supporting organisations and programs targeting the local community;
- Protecting the environment and improve local amenity;
- Attracting and providing infrastructure for commerce, tourism and industry; and
- Managing, improving and developing resources available to the community.

I. How Council collects personal information

Council collects personal information to enable it to conduct its functions. Council assesses the level of personal information that is appropriate to be collected on a case by-case basis. In this section, a reference to personal information is also a reference to health information.

Council collects personal information in a variety of ways including:

- incident reports;
- medical assessment reports;
- submissions;
- application forms;
- CCTV footage;
- financial transaction records;
- contracts;
- customer enquiries and correspondence;
- telematics;
- web services and smart devices; and
- contact tracing under NSW Public Health Orders.

Personal information may be collected from:

- Members of the public;
- NSW public sector agencies;
- Businesses;
- Non-government organisations;
- Employees; and
- Medical professionals.

Contractors acting on Council's behalf may also collect personal information. Council includes clauses in its contracts that require contractors to comply with relevant privacy obligations.

For personal information to be considered 'held by Council', the information must:

- Be in Council's possession or control of; or
- Be in the possession or control of a person employed or engaged by Council during the course of employment or engagement; or
- Be contained in a State record in respect of which Council is responsible under the SR Act.

II. Personal information held by Council

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

- rates records;
- development applications and objections; and
- various types of health information.

Council holds personal information concerning Employees, such as:

- recruitment material;
- leave and payroll data;
- personal contact information;
- performance management information;
- complaints and disciplinary matters;
- pecuniary interest returns;
- wage and salary entitlements; and
- health information, for example medical certificates, workers compensation claims.

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.

III. Privacy and Personal Information Protection Notice

Under section 10 of the PPIP Act, when Council collects personal information from an individual, such as their name, address, telephone number or email address, Council must make the individual aware of:

- The purposes for which the information is being collected;
- The intended recipients of the information;
- Whether the supply of the information is required by law or is voluntary;
- Any consequences for the individual if the information (or any part of it) is not provided;
- Ways the individual can access and correct their personal information; and
- How to contact Council or the Council section that is collecting and holding their information.

In compliance with the PPIP Act, Council includes a Privacy and Personal Information Protection Notice on all forms, letters and documents when collecting personal information from individuals. Council's Privacy and Personal Information Protection Notice appears below.

IV. Storage, access and accuracy of personal information

Personal information is stored electronically and in physical files.

The following applies to information Council holds:

- Only Council employees can access personal information;
- Employees will make every effort to ensure personal information is accurate before using it;
- Employees will use personal information only for the purpose for which it was collected; and
- Employees will not disclose personal information about a person to anyone without the consent of the person it concerns unless they are required or permitted to by law.

Please refer to page 18 for details of exemptions, directions and code of practice that may affect the above.

Electronic information is stored on secure information systems. Networks will be secure and require individual logins. New systems are assessed for compliance with the PPIP Act and HRIP Act. When not being used, hard copy files and sensitive information are securely stored.

Privacy and Personal Information Protection Notice

We are collecting this information to process your request. We may not be able to do so without it. Supplying this information is voluntary and it will not be used for any other purpose without seeking your consent. We will store your personal information on our systems or in our offices, where it will be used by our staff and contractors. Other people can request access to it under the *Government Information (Public Access) Act 2009*.

You can ask us to suppress your personal information from a public register and we will consider your request in line with the *Privacy and Personal Information Protection Act 1998*. Our Privacy Management Plan sets out how you can access or correct your personal information. Please visit www.wentworth.nsw.gov.au for a copy of the plan.

V. Use and disclosure of personal information

Employees use the personal information collected to:

- Deliver services;
- Conduct research;
- Provide advice; and
- Continually improve services.

UNSOLICITED INFORMATION

Unsolicited information is personal, or health information provided to Council in circumstances where Council has not asked for or required the information to be provided. Such information is not deemed to have been collected by Council under Section 10 of the HRIP Act and Section 4(5) of the PPIP Act, but the access, storage, use and disclosure Information Protection Principles in this Plan will apply to any such information, whilst Council continues to hold this information.

Personal information contained in petitions received in response to a call for submissions or unsolicited petitions tabled at Council meetings will be treated the same as any other submission and may be made available for release to the public.

Personal or health information disclosed publicly and recorded for the purposes of webcasting at Council Meetings is not deemed to have been collected by Council. Retention and Use Principles of this information will apply to such information in Council's possession; however, Disclosure Principles will not apply as the information was voluntarily disclosed with the prior knowledge that it would be recorded, broadcast via the internet to the public and made available by Council for public viewing.

PUBLICLY AVAILABLE INFORMATION

Where Council is requested to provide access to, or make a disclosure of, information that has already been published, Council will rely on the provisions of the relevant Act that authorises Council to hold that information and not the PPIP Act (for example, Section 8 of the GIPA Act).

For the purposes of this Plan, publicly available information refers to information or an opinion about an individual, or group of individuals, that is accessible to the general public in any form. It includes information that:

- Has been published or broadcast for public consumption;
- Is openly available on request to the public;
- Is openly accessible on-line or otherwise to the public;
- Is available to the public by subscription or purchase;
- Could be lawfully seen or heard by any casual observer;
- Is lawfully made available at a meeting open to the public; or
- Is obtained by visiting any place or attending any event that is open to the public.

Health information about an individual, or group of individuals, that has been lawfully made accessible to the general public in any form is considered by Council to be 'publicly available information'.

Council views the following information to be publicly available:

- An advertisement containing personal or health information in a local, city or national newspaper (regardless of whether the newspaper is in digital, audio or paper media);
- Personal or health information freely accessible on the internet or on mobile data applications;
- Books or magazines that are printed and distributed to the general public, regardless of the type of media;
- Council business papers in whole or part that are made available to the general public; or
- Personal or health information that may be part of public display on view to the general public.

SUPPRESSION OF INFORMATION AVAILABLE FOR PUBLIC INSPECTION (NOT HELD IN PUBLIC REGISTERS)

Certain material that is made available (or is to be made available) by Council for public inspection by or under the LG Act may be suppressed under section 739 of the LG Act. An application for suppression may be made in circumstances where:

- The material discloses or would disclose a person's place of living; and
- The person concerned considers that the disclosure would place the personal safety of themselves or their family at risk

Requests for suppression should be made in writing to the General Manager and be supported by:

- Information regarding the particulars of the risk; and
- A statutory declaration by the persons(s) making the request or other authorised person.

Requests for suppression may be granted if Council is satisfied that disclosing, or continuing to disclose, the information would place a person or their family members at risk. For more information see section 739 of the LG Act.

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. When in doubt, Council will favour suppression.

Section 739 of the LG Act, however, only applies to material that is publicly available and does not apply to information on a public register.

MANDATORY PROACTIVE RELEASE OF INFORMATION UNDER SECTION 6 OF THE GIPA ACT

Section 6 of the GIPA Act requires that certain government information held by Council must be made publicly available unless there is an overriding public interest against disclosure of the information.

At least one of the ways in which this information is made available must be free of charge.

Section 18 of the GIPA Act requires that Council provide open access to those documents listed under Schedule 1 of the GIPA Regs. In the event of any inconsistencies that exist between the PPIP Act and the GIPA Act, section 57 of the PPIP Act will prevail over clause 1(3) of Schedule 1 of the GIPA Regs.

In other words:

- If a register is listed in Schedule 1 of the GIPA Regs, access must not be given except in accordance with section 57(1) of the PPIP Act;
- If a register is not listed in Schedule 1 of the GIPA Regs, access must not be given except if:
 - It is allowed under section 57(1) of the PPIP Act; and
 - There is no overriding public interest against disclosure of the information under section 6 of the GIPA Act.

PUBLIC REGISTERS

Part 6 of the PPIP Act governs how Council should manage personal information contained in public registers. In this Part, a reference to personal information is also a reference to health information.

A public register is a register of personal information that is required by law to be made, or is made, publicly available or open to public inspection. Access to public registers can be arranged by contacting Council directly.

Public registers generally confer specific rights, privileges, benefits or status in relation to access of certain information by the public which would otherwise not exist.

Council is required by law to maintain a number of public registers and to make them available for public inspection. Some of these registers contain personal information as defined in the PPIP Act, the HRIP Act and the GIPA Act.

Council may, by virtue of its own practice, hold other registers to which the PPIP Act, the HRIP Act and the GIPA Act may apply.

Due to the general emphasis on local government processes and information being open and accountable in accordance with the provisions of the LG Act and the GIPA Act, a secondary purpose for which all public registers are held by Council includes the provision of access to information by members of the public.

Accordingly, disclosure of specific records on public registers would normally be considered permissible under section 57 of the PPIP Act, and persons or organisations who apply to Council to access information contained in any public register for a purpose not related to the primary purpose of the register, may be given access at the discretion of Council.

Any access to information held on a public register mentioned above must be in accordance with the Privacy Code and any other relevant privacy code of practice applicable to the access.

If in doubt, an applicant seeking access to a public register may be requested to provide a statutory declaration to Council to verify their intended use of the information (see Appendix 1).

i. Council's public registers

The GIPA Act and Government Information (Public Access) Act Regulation 2018 (GIPA Regulation) lists information available to the public free of charge within a public register.

The following is a list of Council's public registers:

- Register of Council contracts;
- Register of declarations;
- Register of graffiti removal work;
- Register of gifts and benefits;
- Register of declarations of interest by Councillors;
- Register of declarations of interest by Staff; and
- Register of voting on planning matters.

ii. Disclosure of personal information contained in public registers

Section 57 of the PPIP Act requires Council to ensure that disclosure of personal information in a public register is consistent with, and related to, the purpose for which the register exists.

In line with this requirement (and in accordance with section 2 of the Privacy Code) Council applies specific rules governing disclosure of personal information on public registers, namely:

- Council will not disclose personal information kept in a public register to third parties unless Council is satisfied that the information is to be used for a purpose relating to the purpose of the register, or an Act under which the register is kept;
- The Privacy Code allows disclosure of single items or one page in a public register without explanation. However, such a disclosure may only occur when the person seeking the information attends Council in person;

- Council may require that any person who applies for more than one record or page from a public register does so by completing a Statutory Declaration. Any such declaration must describe the intended use of the information requested and be witnessed by an authorised person such as a Justice of the Peace, lawyer or notary public;
- If the stated purpose of the applicant does not confirm with the purpose or which the public register is kept, access to the information will not be granted; and
- Individuals wishing to inspect Council's pecuniary interest register, or any public register on which records declarations made by Councillors or Designated Officers, may do so without explanation.

iii. Application for access to one's 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.

iv. Suppression of information in relation to a public register

An application for suppression in relation to a public register will be dealt with under section 58 of the PPIP Act.

A person about whom personal information is contained (or proposed to be contained) in a public register, may request Council to:

- Have the information removed from, or not placed on the register as publicly available; and
- Not disclosed to the public.

Requests to suppress information must be submitted in writing to the General Manager and should include the reasons for the request. Council may require supporting documentation be provided where appropriate.

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.

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

Information removed from, or not placed on, a public register may still be retained by Council and used in the exercise of Council functions, but will not be disclosed to other parties.

v. Other registers

Council may have other registers that are not considered public registers. The Information Protection Principles, the PPIP Act, all applicable codes, and this Privacy Management Plan apply to those databases or registers.

HOW TO ACCESS AND AMEND PERSONAL INFORMATION

The PPIP Act and the HRIP Act give people the right to access and amend their personal and health information.

Members of the public should make their request either:

- in person at Council's Administrative Building located at:
26-28 Adelaide Street
Wentworth NSW 2648; or
- to Council's email account:
council@wentworth.nsw.gov.au

or

- in writing, addressed to:
The General Manager
PO Box 81
Wentworth NSW 2648

Council does not charge a fee to access and amend personal and health information.

LIMITS ON ACCESSING AND AMENDING INFORMATION

Council is prohibited from providing access to a person's personal and health information to another person unless:

- A person can give Council consent to collect their personal information from, or disclose their personal information to, someone that would not normally have access to it (section 26 of the PPIP Act refers);
- The use and disclosure of personal information is permitted under the Privacy Codes of Practice (refer to Exemptions, directions and codes of practice for details);
- That person is an "authorised person", who can act on behalf of someone else in regards to their health information (sections 7 and 8 of the HRIP Act refers); or
- Council is authorised to provide the information at the request of the person to whom it concerns or in the event to lessen or prevent a serious and imminent threat to the life, health and safety of the individual (Clause 11 Schedule 1 of the HRIP Act).

DATA BREACHES

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to Council's physical or electronic information or data, such as:

- accidental loss or theft of information or equipment on which such information is stored;
- unauthorised use, access to or modification of data or information systems to gain unauthorised access or make unauthorised changes to data or information;
- accidental or unauthorised disclosure of personal information (e.g. email containing personal information sent to incorrect recipient);
- personal information published or posted on Council's website without consent;

- access to data by an authorised user for unauthorised reasons (e.g. an employee looking up information in a system for personal reasons in breach of the Code of Conduct);
- accidental disclosure of user login details through phishing;
- malware infection; or
- disruption to or denial of IT services.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of personal information.

I. How we will manage a data breach

The Director – Finance & Policy will be promptly informed of any data breach and will assist in the assessment and management of the breach, including any reporting under NSW's voluntary data breach reporting scheme, in accordance with the Information and Privacy Commission's Voluntary Data Breach Notification guidelines.

Council will determine the seriousness of a breach by:

- Considering the type of data released;
- Whether personal or health information was disclosed;
- The number of individuals affected; and
- The risk of harm that could be caused to individuals, organisations and/or Council by the breach.

After the seriousness of a breach has been determined, Council will take the following steps to manage a data breach:

- **Contain** – steps will be taken to contain the breach and minimise any resulting damage.
- **Evaluate** – ascertain the type of data involved in the breach and the risks associated with the breach. This will include an assessment of who is affected by the breach, what was the cause of the breach, and any foreseeable harm to the affected individuals/organisations.

- **Notify** – individuals/organisations affected by the breach will be notified as soon as possible to enable them to take any steps required to protect themselves, and to advise them of their rights to lodge a complaint with the Privacy Commissioner. Council's default position is to voluntarily report data breaches of personal information to the Privacy Commissioner.
- **Act** – any additional action identified to mitigate risks will be implemented.
- **Prevent** – preventive efforts will be put into action based on the type and seriousness of the breach.

II. Mandatory Notification of Data Breach (MNDB) scheme

A Mandatory Notification of Data Breach (MNDB) Scheme will come into effect on 28 November 2023. This will require Council to satisfy other data management requirements including to maintain an internal data breach incident register and have a publicly accessible data breach policy.

The MNDB scheme will apply to data breaches that involve personal information or health information and where a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates. Under the scheme Council will be required to notify the Privacy Commissioner and the affected individual of eligible data breaches.

Council's Data Breach Policy will be published on Council's website and will describe the procedures and practices used by Council to ensure compliance with the obligations and responsibilities set out in PART 6A for the mandatory notification of data breach scheme.

REVIEW RIGHTS AND THE COMPLAINTS PROCESS

Council encourages individuals to try to resolve privacy issues with us informally before going through the formal review process to allow speedier resolution of concerns. Any person who may have a privacy concern can contact Council by phone for advice or for referral to the Public Information Officer. Alternatively write or email Council with any concerns and Council will respond providing advice on the best course of action.

The informal complaints resolution process may involve a variety of actions including (but not limited to) formal or informal meetings, mediation and/or consultation with parties to the complaint.

At any time during the process, a complainant may elect to lodge a request for an internal review of their complaint.

If at the conclusion of the informal process, the complainant is dissatisfied with the outcome of the process, they may lodge a request for an internal review of their complaint.

i. Internal Review

Under section 53 of the PPIP Act, any individual who is aggrieved by the conduct of Council, or Council staff, in relation to the manner in which their personal or health information is collected, stored, used, accessed, amended, disclosed or destroyed is entitled to apply for a review of that conduct.

The Public Information Officer or their delegate will conduct the internal review. If the internal review is about the conduct of the Public Information Officer, the General Manager will appoint another person to conduct the internal review. The reviewing officer will refer to the Privacy Commissioner's guidance materials when carrying out an internal review.

Council will acknowledge receipt of an internal review application within 5 working days and complete an internal review within 60 calendar days.

Once the review is completed, Council may take no further action, or it may do one or more of the following:

- make a formal apology;
- take remedial action;
- provide undertakings that the conduct will not occur again; or
- implement administrative measures to reduce the likelihood of the conduct occurring again.

Within 14 calendar days of completing an internal review, Council will notify the applicant of the following:

- the findings of the review;
- the action proposed to be taken by Council and the reasons for taking that action (if any); and
- the right of the applicant to have those findings, and Council's proposed action, administratively reviewed by the NSW Civil and Administrative Tribunal.

ii. The role of the Privacy Commissioner in the review process

The Privacy Commissioner has an oversight role in how privacy complaints are handled and is entitled to make submissions to Council regarding internal reviews.

If Council receives an internal review application, it will:

- notify the Privacy Commissioner of the application as soon as practicable;
- keep the Privacy Commissioner informed of the progress of the internal review; or
- inform the Privacy Commissioner of the findings of the review and the action proposed to be taken by Council in relation to the matter.

An individual can also make a complaint directly to the Privacy Commissioner about an alleged breach of their privacy.

iii. External review by the NSW Civil and Administrative Tribunal (NCAT)

If an internal review is not completed within 60 days, or the applicant is not satisfied with the findings of an internal review or the action taken by Council in relation to the review, the applicant has the right to seek an external review and may make application to the NSW Civil and Administrative Tribunal (NCAT) for a review of Council's conduct.

An application for external review can only be made after an internal review has been completed and must be made within 28 days from the date of the internal review decision.

Under section 45 of the PPIP Act, individuals may lodge a complaint directly with the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual and where the conduct involves:

- The contravention by Council or Council staff of an information protection principle that applies to Wentworth Shire Council;
- The contravention by Council or Council staff of a privacy code of practice that applies to Wentworth Shire Council; or
- The disclosure by Council or Council staff of personal information kept in a public register.

Complaints may be lodged in writing or verbally, however individuals may be requested to put any verbal complaint in writing.

Complaints should be made within six (6) months of the complainant first becoming aware of the conduct or matter that is subject of the complaint.

Complaint may be withdrawn or amended, at any time.

PROMOTING PRIVACY

i. Compliance Strategy

During induction, and on a regular basis, all employees will be made aware of this Plan and it will be made available on Council's Intranet and Council's website.

Council officials will be regularly acquainted with the general provisions of the PPIP Act and HRIP Act and, in particular, this Plan, the Information Protection Principles, the Public Register provisions, the Privacy Code of Practice for Local Government, and any other applicable Code of Practice.

ii. Communication Strategy

Council will promote awareness of this plan and rights under PPIP Act, HRIP Act and this Plan to Council officials by:

- Providing an overview at inductions and including a copy of the plan in induction packs;
- Publishing the plan on our internal and external websites;
- Offering training sessions on a regular basis as required;
- Providing specialised and on-the-job training to key groups; and
- Promoting the plan regularly through newsletters, all staff emails, online staff forums and initiatives such as Privacy Awareness Week.

iii. Promoting the Plan to the Community

Council promotes public awareness of this Plan to the community by:

- Making it publicly available and publishing it on our website;
- Writing the Plan in plain English;
- Telling people about the Plan when they enquire about personal and health information;
- Provide a link on our website to the Information & Privacy Commission website and distributing copies of literature available on that site;
- Including privacy statements on application forms and invitations for community engagement; and
- Publishing a Privacy Handout advising how to access information on an individual's rights under PPIP Act, HRIP Act and this Plan.

Privacy & other legislation

This section contains a general summary of how Council must manage personal and health information under the PPIP Act and HRIP Act and other relevant laws.

PPIP Act provides for the protection of personal information by means of twelve (12) Information Protection Principles (IPPs) and HRIP Act provides for the protection of health information by means of fifteen (15) Health Privacy Principles (HPPs)

The way in which Council complies with the IPPs and HPPs are set out below.

1. COLLECTION OF PERSONAL INFORMATION FOR LAWFUL PURPOSES (IPP 1 & HPP 1)

Council will only collect personal information and/or health information for a lawful purpose as part of its proper functions and activities as governed by the LG Act, guidelines issued by the Office of Local Government (OLG) and the IPC, and relevant state and federal legislation.

The compilation or referral of registers and/or rolls are the primary means by which Council collects personal and/or health information about, or from, an individual.

Council may collect information from or share information with other agencies in accordance with legislative requirements, memorandums of understanding or referral arrangements. Council does have legislative requirements in this regard and these include collecting / sharing information with agencies including but not limited to NSW Land Registry Services, NSW Valuer General, NSW Electoral Commission and the NSW Ombudsman for property related matters and enquiries.

Other means include forms that customers complete and lodge with Council for the purposes of development consent, companion animal registration, applications for specific inspections or certificates, or venue bookings.

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

Such personal and health information may include names, residential address, phone numbers, email addresses, signatures, medical certificates, photographs and video footage (CCTV).

Council staff, and anyone engaged by Council (including consultants and contractors), who undertake the collection of personal and/or health information for any reason, must not collect such information by any unlawful means. This includes any debt recovery actions undertaken by an external service provider on behalf of Council.

Where Council requires an individual to provide their personal information (whether this be by submission of a form or written request application) the individual must be provided with a copy of, or link to Council's Privacy Statement.

Any new, amended, or alternative forms, notices or application requests through which personal and/or health information is, or will be, collected by Council will be referred to the Public Information Officer for consideration and review prior to adoption or use to ensure compliance with all Privacy Principles and this Plan.

In the event that any doubt exists as to a form or document's compliance with the Privacy Principles, the opinion of the Public Information Officer will be sought. In the event that concerns are of a legal nature, the matter may be referred to Council's legal advisor.

The Public Information Officer may also provide advice on:

- Whether the collection of the personal or health information is for a lawful purpose;
- Whether the lawful purpose is directly related to a function or activity of Council;
- Whether or not the collection of the personal or health information is reasonably necessary for the lawful purpose

There are no exemptions from IPP 1 & HPP 1 under the Privacy Code or PPIP Act or the HRIP Act.

2. COLLECTION OF PERSONAL INFORMATION DIRECTLY FROM THE INDIVIDUAL (IPP 2 & HPP 3)

Personal information will be collected directly from the individual, unless:

- That person authorises in writing the collection of the information from another person; or
- In the case of person under the age of 16 years, the information is being provided by a parent or guardian of the person; or
- In the case of a person over the age of 16 years and who is subject to a lawful guardianship order, the information is being provided by the guardian of the person and satisfactory evidence of guardianship has been provided to Council.

Health information will be collected:

- Directly from the person concerned, unless it is unreasonable or impracticable to do so; and
- In accordance with any guidelines issues by the Privacy Commissioner for the purposes of this clause.

Collection of information may occur via phone, written correspondence to Council, email, facsimile, electronic and paper based forms, video or data recordings, mobile applications or in person.

Personal and/or health information will only be collected by Council in circumstances where:

- The collection of the information is relevant and necessary for the proper exercise of Council's functions;
- The collection of the information is required by law;
- The collection of the information is reasonable, appropriate and justifiable; and
- The collection of the information is lawful.

Exemption(s) for IPP 2

Compliance with IPP 2 is subject to certain exemptions under the PPIP Act and the Privacy Code. If one of these exemptions apply, Council need not comply with the provisions of IPP 2. The exemptions will only be relied upon in very obvious and limited circumstances and legal advice should normally be obtained. The exemptions include:

- Privacy Code where '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';
- Section 23(2) of the PPIP Act where the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal;
- Section 24(6)(a) of the PPIP Act where Council is collecting information in connection with the investigation or otherwise handling of 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;
- Section 25(a) of the PPIP Act where Council is lawfully authorised or required to not comply with this principle under an Act or any other law. This includes where information is collected from other public sector agencies under a statute or law;
- Section 25(b) of the PPIP Act where non-compliance is 'necessarily implied' or 'reasonably contemplated' under any Act or law;
- Section 26(1) of the PPIP Act where compliance would prejudice the interests of the individual to whom the information relates;
- Section 27A of the PPIP Act where:
 - The collection is for the purpose of

providing the information to another public sector agency or the collection by Council is from another public sector agency; and

- The collection is reasonably necessary for Council to deal with, or respond to correspondence from a Minister or member of Parliament; or to enable inquiries to be referred between Council and other public sector agencies; or to enable the auditing of the accounts or performance of Council.
- Section 27B of the PPIP Act where:
 - The collection is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest; and
 - It is unreasonable or impracticable for the information to be collected directly from the individual to whom the information relates.

There are no exemptions from HPP 3.

3. REQUIREMENTS WHEN COLLECTING PERSONAL INFORMATION (IPP 3 & 4 and HPP 2 & 4)

Before personal or health information is collected by Council, or as soon as practicable after collection, Council will provide individual(s) with a copy of Council's Privacy Statement and will take reasonable steps to ensure that the individual to whom the information relates is aware:

- That the information is being collected;
- The purpose for which the information is being collected;
- The persons to whom (or types of persons to whom) the organisation may disclose the information;
- Whether the supply/provision of information from the individual is required by law or is voluntary;
- Any consequences for the individual if all or any of the information is not provided or supplied;

- The department, section or location within Council where the information will be held or stored;
- The existence of any right to access and/or correct the information; and
- Council's address and contact information.

Council will ensure that any personal or health information collected about individuals will be relevant to the purpose for which it is collected, not excessive, accurate, up to date and complete. Various sections of this Plan provide specific guidance and advice in relation to how Council will ensure accuracy, relevancy and legitimate purpose requirements are to be met.

Council will ensure that the collection of any personal or health information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates by complying with the relevant clauses of this Plan.

Where Council collects health information about an individual from a third party, Council will take reasonable steps to ensure that the individual is aware of the matters discussed in this Plan unless:

- Making the individual aware would pose a serious threat to life or health of any individual; or
- The collection is made in accordance with guidelines issued by the Privacy Commissioner.

Closed Circuit Television (CCTV)

Council may use public place video surveillance in accordance with the NSW Government policy statement and guidelines for the establishment and implementation of closed circuit televisions (CCTV) in public areas.

The use of CCTV and other forms of surveillance by Council is subject to the provisions of the *Workplace Surveillance Act 2005*. Council ensures compliance with these provisions by:

- Strictly limiting and monitoring access to any CCTV footage held by Council. Access to CCTV will not be granted without prior written authorisation of the relevant Director or the General Manager;
- Council officers responsible for the custody, storage and security of any CCTV must be provided with written authorisation from the relevant Director or the General Manager before providing access to any CCTV and maintain a diary record or log of each occasion when access to any footage is provided;
- Maintaining a register of all cameras utilised by Council;
- Requiring executive approval for access to any material obtained through CCTV or other form of surveillance;
- Notifying Council staff of any surveillance (other than authorised covert surveillance) conducted in the workplace. Notification includes:
 - The type of surveillance;
 - How the surveillance will be carried out;
 - When the surveillance will start and finish (if applicable);
 - Whether the surveillance will be continuous or intermittent; and
 - Whether the surveillance will be ongoing or for a limited period
- Using signage to notify all individuals (Council staff and members of the public) who enter Council premises that CCTV are in use and that they may be incidentally filmed during their attendance;

- Implementation of an internal investigation procedure that strictly controls how any covert surveillance may be undertaken. Covert surveillance may not be undertaken without a covert surveillance authority being issued to Council by a magistrate and the express written authorisation of the General Manager;
- Restricting where CCTV may be placed to ensure that no CCTV surveillance is undertaken in any prohibited area (for example toilets, change rooms and so on);
- Any Council officer found to be accessing, storing, using or disclosing CCTV footage outside of Council policies and procedures or in breach of the *Workplace Surveillance Act* may be subject to disciplinary action.

Exemption(s) for IPP 3

Compliance with IPPS 3 is subject to certain exemptions under the PPIP Act and the Privacy Code. If one of these exemptions apply Council need not comply with IPP 3. The exemptions will be relied upon only in very obvious and limited circumstances and legal advice should normally be obtained. The exemptions include:

- Privacy Code where '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';
- Section 23(3) of the PPIP Act where information is collected for law enforcement purposes. Note that protections provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence are not removed or amended by this exemption;
- Section 24(6)(a) of PPIP Act – where Council 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;

- Section 25 of PPIP Act – where Council is lawfully, authorised, permitted or required to not comply with IPP 3;
- Section 26 of PPIP Act – where the collection of information by Council would prejudice the interests of the individual to whom the information relates, or if the individual to whom the information relates has provided their express consent to Council not to comply with IPP 3;
- Section 27A of the PPIP Act where:
 - The collection is for the purpose of providing the information to another public sector agency or the collection is from another public sector agency; and
 - The collection is reasonably necessary for Council to deal with, or respond to correspondence from a Minister or member of Parliament; or enable inquiries to be referred between Council and other public sector agencies; or to enable the auditing of the accounts or performance of Council.
- Section 27B of the PPIP Act where:
 - The collection is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest; and
 - It is unreasonable or impracticable for the information to be collected directly from the individual to whom the information relates.

There are no exemptions for IPP 4 under the Privacy Code or PPIP Act. There are no exemptions for HPP 2 under the HRIP Act.

Exemption(s) for HPP 4

Non compliance with HPP 4 is permitted if:

- The person to whom the information relates has expressly consented to Council not complying; or
- Council is lawfully authorised, required or

permitted to not comply under an Act or any other law; or

- Compliance would prejudice the interests of the individual to whom the information relates; or
- The information is collected for law enforcement purposes; or
- Compliance might detrimentally effect (or prevent the proper exercise of) Council's compliant handling functions or any of its investigative functions in relation to a matter that could be referred or made to an investigative agency, or that has been referred from an investigative agency (see HPP 4 – (7) for more information).

If the health or personal information relates to a minor, a person subject to a guardianship order, or a person who Council reasonably believes incapable of understanding the matters discussed under this section of the Plan, Council will take reasonable steps to ensure any authorised representatives of the individual is aware of those matters;

In accordance with this Plan, a Privacy Statement has been published on Council's website, intranet site, as a publicly available handout and included on Council forms where personal or health information of individuals is collected.

4. RETENTION, DESTRUCTION AND SECURITY OF PERSONAL INFORMATION (IPP 5 & HPP 5)

Disposal and destruction of documents will be in accordance with the relevant authority document issued by State Records NSW.

Personal and health information collected by Council will be retained for no longer than as required by:

- General retention and disposal authority: local government records (GA39); and/or
- General retention and disposal authority: administrative records (GA28); and/or
- General retention and disposal authority:

audio visual programs and recordings (GDA11);

- General retention and disposal authority: original or source records that have been copied (GA45);
- General retention and disposal authority: source records that have been migrated (GA48); and/or
- General retention and disposal authority: video/visual surveillance records created by NSW public offices (GDA8).

Council will undertake reasonable security safeguards to ensure that all personal and health information of individuals is secured and stored in a manner that will protect the information against loss, misuse, unauthorised access, use, disclosure, modification or destruction. Such safeguards shall include (but is not limited to) restricted access to information, password protection for IT accounts, electronic swipe cards for physical security and authorisation protocols and procedures for access approvals.

Council will implement, monitor and maintain specific policies and procedures (however titled) relevant to the safeguard and security of personal and health information.

Council staff are required to undertake training in Council's records management and IT security policies and procedures and ensure they understand their obligations in relation to the safety, security, use, access, storage and destruction of all records held by Council, including personal and health information.

Council staff will be provided access to information according to the duties of the position which they undertake. Access to information not relevant to their position will be restricted and will require the written approval of the relevant Director responsible for the supervision of the individual concerned.

Individuals who breach any policy or procedure designed to safeguard personal and health

information held by Council may be subject to disciplinary or other action as appropriate and/or may be subject to penalties under the PPIA Act, HRIP Act or the *Crimes Act 1900*.

If it is necessary for personal or health information to be given to a person or persons in connection with the provision of a service to Council (for example consultants and contractors), all reasonable steps will be undertaken by Council to prevent the unauthorised use or disclosure of the information by such person or persons. Reasonable steps may include (but is not limited to) training as appropriate, provision of relevant Council policies and procedures, restrictions on access, direct supervision, appropriate terms in contractual agreements and so on.

There are no exemptions for IPP 5 under the Privacy Code or PPIP.

Exemption(s) for HPP 5

Non-compliance with HPP 5 is permitted under the following circumstances:

- Council is lawfully authorised or required to not comply with HPP 5; or
- Non-compliance is permitted under an Act or any other law.

5. TRANSPARENCY AND ACCESS (IPP 6 & 7 AND HPP 6 & 7)

Council will take reasonable steps to enable any person to ascertain:

- Whether Council holds personal and/or health information; and
- Whether Council holds any personal and/or health information relating to that person; and
- The nature of the information held;
- The purpose for which the information is used; and
- The person's entitlement to gain access to the information held.

As a matter of practicality, not every item of personal information, however insignificant will be capable of ascertainment.

Individuals who request access to their personal and/or health information held by Council should be provided access without excessive delay or expense.

Under section 20(5) of the PPIP Act, access to personal information is subject to any applicable conditions or limitations contained in the GIPA Act

Individuals may access their personal and/or health information by either:

- Making an application in writing to access their personal or health information under either the PPIP Act or HRIP Act (as appropriate) by writing to the Public Information Officer and submitting their request.
- Making an application in writing to access their personal or health information under the GIPA Act by completing an “informal Access to Information Request form” located on Council’s website and submitting it to Council.

Access to information applications under the PPIP Act or HRIP Act should include the following information:

- Name, address and contact details of person making the application (including email address, phone number and so on);
- Particulars of information required (including nature of information, relevant date/time period, type of record – for example paper and/or digital);
- The type of access sought (for example view access, paper copies, electronic copies);
- Supporting documentation where required (for example third party authorisation); and
- Individuals may also be required to provide proof of identity before any information will be released.

Access to information applications under the GIPA Act are typically handled under the informal access provisions of the GIPA Act.

In certain limited circumstances, individuals may be requested to lodge a Formal Access to Information Request lodged if the initial request is unable to be dealt with through the informal access process.

In responding to requests, Council will undertake a search for records relevant to the request and may seek additional information from the Applicant to assist the search.

Applicants may be requested to pay a fee in accordance with the provisions of section 66B of the PPIP Act for information relating to:

- A copy of their health information;
- An opportunity to inspect and take notes of the health information;
- Amending health information at the request of the applicant.

Requests to access personal information may also be subject to fees payable under the GIPA Act (for example records relating to suitability for employment as a public sector employee, performance appraisals and so on).

Exemption(s) for IPP 6 and IPP 7

Compliance with IPPs 6 & 7 is subject to certain exemptions under the PPIP Act and the Privacy Code. The exemptions will be relied upon only in very obvious and limited circumstances and legal advice should normally be obtained. The exemptions include:

- IPP 6 & 7 – section 24(6)(a) of the PPIP Act in circumstances where Council is investigating or 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;
- IPP 6 & 7 – section 25 of the PPIP Act where non-compliance is lawfully authorised, permitted or required under an Act or any other law;
- The provisions of the GIPA Act that impose conditions or limitations with respect to IPP 6 and/or 7 apply and may

modify or amend Council's compliance obligations for these principles.

Exemption(s) for HPP 6 & 7

Non-compliance with HPP 6 and HPP 7 is permitted under the following circumstances:

- Council is lawfully authorised or required to not comply; or
- Non-compliance is permitted under an Act or any other law.

6. ALTERATION, MODIFICATION OR AMENDMENT OF PERSONAL INFORMATION (IPP 8 & HPP 8)

Council will at the request of a person, allow appropriate amendments (including corrections, deletions or additions) to be made to the personal and/or health information held by Council.

Alterations to information held should ensure that the information is accurate, relevant, up to date, complete, not misleading and appropriate to the purpose for which the information was collected.

Requests for alterations must be made in writing (as set out above in the Plan) and accompanied by satisfactory supporting evidence. Council may, at any time, request additional evidence or information in determining the request.

There is no fee applicable to a request for an alteration to personal or health information held by Council. Where requested, and provided that it is reasonably practicable, amendments to personal information will be notified by Council to ordinary recipients of that information.

In circumstances where Council is not prepared to amend personal information in accordance with a request, Council must (at the request of the person concerned) attach to the relevant (unamended) record any statement provided by the person requesting the amendment of the record. The statement should be attached in such a way that it can be easily read in conjunction with the unamended record.

Changes of information relating to the legal name of the person, residential address and/or other minor amendments require appropriate supporting documentation and identification verification.

Where there are complaints that are, or could be, the subject of a staff complaint or grievance, they will be referred to the Manager Human Resources in the first instance and treated in accordance with Council's Complaint Management Framework.

Any alterations to personal information that are, or could be, the subject of a customer complaint or grievance will be referred to the Public Information Officer, who will make a recommendation in relation to the matter.

Where Council is conducting an investigation, it will have regard to any applicable Direction of the Privacy Commissioner under section 41 of the PPIP Act that may affect the application of IPP 8. There are no exemptions for IPP 8 under the Privacy Code or the PPIA Act.

Exemptions for HPP 8

Non-compliance with HPP 8 is permitted under the following circumstances:

- Council is lawfully authorised or required to not comply; or
- Non-compliance is permitted, necessarily implied or reasonably contemplated under an Act or any other law.

7. ACCURACY OF INFORMATION CHECK BEFORE USE (IPP 9 & HPP 9)

Council will take all reasonable steps necessary to ensure personal and health information is accurate, relevant, complete, not misleading and up to date before using the information.

In undertaking checks, Council will take into account the age of the information, its significance, the likelihood of change and the particular function for which the information was collected.

The more significant the information, the greater the necessity that checks for accuracy and currency are undertaken prior to its use. For example, employee records should be updated when there is any change of circumstance or when the employee's contact details change.

In checking the accuracy of information before use Council may:

- Cross reference information from multiple sources/systems to verify consistency, reliability and uniformity of the information;
- Request verification of the information from the individual/organisation to whom the information relates;
- Request verification of the information from a trusted source – for example a statutory/regulatory authority (where appropriate);
- Consider if the information is credible, reasonable, unbiased and supported by reliable evidence;
- Determine if there is any conflict of interest relevant to the originating source of the information;
- Take steps to verify if the source of the information is a primary or secondary source;
- Take steps to verify that the information has not been altered, tampered with, or amended in any unauthorised manner since collection of the information. For example, comparing the information with an original/ source document; or
- Review the audit history of electronic information to determine when, where, how and by whom information was accessed, amended, altered, added or updated.

Checks for accuracy of information must be undertaken in the following circumstances:

- Whenever critical, sensitive or personal information is determined to be incomplete, partial or misleading;
- Whenever critical, sensitive or personal information is to be collected, accessed,

used or disclosed;

- Whenever critical information necessary for the functions of Council is to be updated, altered, or amended (for example contact details of employees, property owner information following sale of rateable land and so on);
- Whenever information is to be relied upon for decision making by Council;
- Whenever information is to be transferred from one storage system to another (for example when hard copy records are transferred to a digital electronic storage system);
- Whenever information is to be used for a purpose other than the primary purpose for which it is collected;
- Whenever information held by Council is to be transferred to another jurisdiction, agency or entity;
- Whenever information is required by law (for example under subpoena or statutory reporting); or
- Whenever system alerts for information review are triggered include automatic alerts in relation to expiry of information, destruction dates of information, creation dates of information and collection dates of information.

Procedures for maintaining, reviewing and ensuring the accuracy of information held by Council are detailed in Councils Records and Information Management Policy.

There are no exemptions for IPP 9 under the Privacy Code or PPIP Act.

There are no exemptions for HPP 9 under the HRIP Act.

8. LIMITS ON USE OF PERSONAL INFORMATION (IPP 10 AND HPP 10)

Personal and health information collected by Council will only be used for the purpose(s) for which it is collected (the primary purpose) and not for any other purpose(s) (secondary purpose) unless:

- The individual to whom the information relates has expressly consented to the use of the personal or health information for that secondary purpose; or
- The secondary purpose is directly related to the primary purpose, and the individual would reasonably expect that Council would use the personal or health information for the secondary purpose; or
- The use of the personal or health information is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of a person; or a serious threat to public health or safety.

The Privacy Code makes provisions that Council may use personal information for a secondary purpose in circumstances 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). For example, Council rates records held under section 602 of the *Local Government Act 1993* may also be used to notify neighbours of a proposed development, evaluate a road opening;
- The information is to be used for the purpose of conferring upon a particular individual an award, prize, benefit or similar form of personal recognition.

In addition to the above, health information collected by Council may be used for a secondary purpose in circumstances where:

- The use of the health information is necessary for the funding, management planning or evaluation of health services and is in accordance with the provisions of HPP 10 (1)(d);

- The information is reasonably necessary for the training of employees of Council or other persons working with Council (such as consultants and/or contractors) as prescribed by HPP 10 (1)(e);
- The use of the information is reasonably necessary for research, is in the public interest and is in accordance with the provisions of HPP 10 (1)(f);
- The use is related to a law enforcement agency ascertaining the whereabouts of a missing person;
- The use is necessary for the purpose of an investigation into, or reporting of, suspected unlawful activity, unsatisfactory professional conduct, professional misconduct, or conduct subject to disciplinary action as prescribed by HPP 10(1)(h); or
- The use is necessary for the purpose of Council investigating or handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred to Council from or made by an investigative agency.

Where Council is conducting an investigation, it will have regard to any applicable direction of the Privacy Commissioner under section 41 of the PPIP Act that may affect the application of IPP 10.

Exemption(s) from IPP 10

Permitted non-compliance with IPP 10 exists under:

- Section 23(4) of the PPIP Act which allows Council to use personal information in circumstances where it is reasonably necessary for law enforcement purposes or for the protection of public revenue;
- Section 24(2) of the PPIP Act (as authorised by section 26(a)) where the secondary use of the information is reasonably necessary in order to enable Council to exercise its complaint handling functions or any of its investigative functions;

- Section 25 of the PPIP Act where the use of the personal information is lawfully authorised, required, permitted, necessarily implied or reasonably contemplated under an Act or any other law;
- Section 27A of the PPIP Act where:
 - Collection is for the purpose of providing the information to another public sector agency or collected by Council from another public sector agency; and
 - Collection is necessary for Council to deal with, or respond to correspondence for a Minister or Member of Parliament; or to enable inquiries to be referred between Council and other public sector agencies or to enable the auditing of the accounts or performance of Council.
- Section 27B of the PPIP Act where:
 - The use of the information is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest; and
 - The purpose cannot be served by using information that does not identify the individual, or from using information from which the individual's identity cannot be reasonably ascertained, and it is impractical for Council to seek the consent of the individual for the use or disclosure; or
 - Reasonable steps are taken to de-identify the information before use, and (where the information could reasonably be expected to identify individuals) the information is not published in a publicly available publication; and
 - The use of the information identified above must always be in accordance with guidelines, if any, issued by the Privacy Commissioner.
- Section 28(3) of the PPIP Act where the disclosure is:
 - By Council to another public sector agency (or vice versa) under the administration of the same Minister and the purpose is that of informing that

Minister about any matter within the administration; or

- By another public sector agency to Council (or vice versa) under the administration of the Premier if the disclosure is for the purposes of informing the Premier about any matter.

Exemption(s) from HPP 10

Permitted non-compliance with HPP exists in circumstances where:

- Council is lawfully authorised or required to not comply;
- Non-compliance is permitted, necessarily implied or reasonably contemplated under an Act or any other law;
- the use is for the purpose of a disclosure by Council to another public sector agency under the administration of the Minister for Local Government (for example the Office 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 (HPP 10(4)); or
- the use is necessary for the purpose of Council investigating or handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred to Council from or made by an investigative agency as per HPP 10(5).

9. RESTRICTIONS AND LIMITS ON DISCLOSURE OF PERSONAL INFORMATION (IPP 11 & HPP 11)

Council will only disclose personal and/or health information in circumstances where:

- The individual has expressly consented to the disclosure; or
- The individual was informed at the time of collection that Council would be disclosing the information to specific recipients; or
- The disclosure is for a related purpose(s) and Council has no reason to believe that the person would object to the disclosure; or
- The disclosure is for a related purpose(s) and it is likely that the person would reasonably expect that Council would disclose the information for the related purpose; or
- The disclosure is necessary in order to deal with a serious and imminent threat to a person(s) life, health and safety or to public health and safety.

Related purposes may include (but are not limited to):

- Disclosure of information for the delivery of a service by another person or agency that supplements a service(s) provided by Council; or
- Disclosure of information to a third party for the purpose of assessment or review of the delivery of a program or service to which the original collection of information relates.

Third party's (such as Contractors and Consultants) are subject to Council's third party IT Access protocols and must comply with the following:

- Access to Council records must be in accordance with any restrictions imposed by Council;
- Utilisation of Council's systems must not contravene any Council policy, procedure,

Code of Conduct and/or relevant legislation;

- Council reserves the right to monitor and examine all records stored in, or transmitted by, Council computers, and network or communication devices; and
- Passwords and account logins must not be shared with any other person.

Where Council is conducting an investigation, any disclosure of information will have regard to any applicable direction of the Privacy Commissioner under section 41 of the PPIP Act.

In addition to the above, health information collected by Council may also be disclosed for a secondary purpose in circumstances where:

- The information is genetic information and the disclosure is to a genetic relative of the individual;
- The disclosure is necessary for the funding, management planning or evaluation of health services as prescribed by HPP 11 (1) (d); or
- The disclosure is necessary for the training of employees of Council or other persons working with Council (such as consultants and/or contractors) as prescribed by HPP 11 (1)(3); or
- The disclosure is reasonably necessary for research, is in the public interest and is in accordance with the provisions of HPP 11 (1)(f); or
- The disclosure is reasonably necessary to provide information to an immediate family member of the individual for compassionate reasons as prescribed by HPP 11 (1)(g); or
- The disclosure is related to a law enforcement agency, or an organisation authorised by the HRIP regulations, ascertaining the whereabouts of a missing person; or
- The disclosure is necessary for the purpose of a Council investigation into, or reporting of, suspected unlawful activity, unsatisfactory professional conduct, professional misconduct, or conduct subject

- to disciplinary action; or
- The disclosure is reasonably necessary for the exercise of law enforcement where there are reasonable grounds to believe that an offence may have been, or may be committed; or
- The disclosure is necessary for the purpose of Council investigating or handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred to Council from or made by an investigative agency.

If personal or health information is disclosed to a person or body that is a public sector agency in accordance with this Principle, that person or agency must not use, or disclose, the information for any purpose other than the purpose for which the information was provided.

Exemption(s) for IPP 11

Permitted non-compliance with IPP 11 exists under:

- Section 23(5)(a) of the PPIP Act where disclosure is made to a law enforcement agency in connection with proceedings for an offence or for law enforcement purposes. However, Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or lawful requirement;
- Section 23(5)(b) of the PPIP Act where 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 PPIP Act where disclosure is authorised by subpoena, search warrant, or other statutory instrument;
- Section 23(5)(d) of the PPIP Act where disclosure:
 - Is reasonably necessary for the protection of public revenue (for example a fraud with respect to taxed 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; or
- Is reasonably necessary to investigate an offence where there are reasonable grounds to believe an offence has been committed.
- Section 23(6A) of the PPIP Act where:
 - Council is disclosing the information to another public sector agency or is receiving information from another public sector agency; and
 - The disclosure is reasonably necessary for law enforcement purposes.
- Section 23(7) of the PPIP Act where the disclosure of the information concerned is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed.
- Section 24(6)(a) of the PPIP Act where:
 - Compliance may detrimentally affect Council's complaint handling or investigative functions;
 - The information is disclosed to another investigative agency;
 - Non-compliance is reasonably necessary to assist another public sector agency that is an investigative agency in exercising its investigative functions;
 - The information is disclosed to a complainant and the disclosure is reasonably necessary for reporting the progress of an investigation into the complaint or providing the complainant with advice as to the outcome of their complaint or any action taken as a result of the complaint;
 - Council is handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred to Council from an investigative agency.

- Section 25 of the PPIP Act where non-compliance is lawfully authorised, required, permitted, necessarily implied or reasonably contemplated under an Act or any other law.
- Section 26(2) of the PPIP Act where an individual expressly consents to Council not complying with IPP 11.
- Section 27A of the PPIP Act where:
 - The disclosure is for the purpose of providing the information to another public sector agency or the disclosure to Council is from another public sector agency; and
 - The disclosure is reasonably necessary for Council to deal with, or respond to correspondence from a Minister or member of Parliament; or to enable inquiries to be referred between Council and other public sector agencies; or to enable the auditing of the accounts or performance of Council.
- Section 27B of the PPIP Act where:
 - The disclosure of the information is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest; and
 - The purpose cannot be served by disclosing information that does not identify the individual, or from disclosing information from which the individual's identity cannot be reasonably ascertained, and it is impractical for Council to seek the consent of the individual for the disclosure of the information; or
 - Reasonable steps are taken to de-identify the information before disclosure, and (where the information could be reasonably be expected to identify individuals) the information is not published in a publicly available publication; or
 - The disclosure of information mentioned above must always be in accordance with guidelines, if any, issued by the Privacy Commissioner.

- Section 28(3) of the PPIP Act where the disclosure is:
 - By Council to another public sector agency (or vice versa) under the administration of the same Minister and the purpose is that of informing that Minister about any matter within the administration; or
 - By another public sector agency to Council (or vice versa) under the administration of the Premier if the disclosure is for the purpose of informing the Premier about any matter.

The Privacy Code also makes provision that Council may use personal information for a secondary purpose in circumstances where:

- The disclosure is to a public sector agency or public utilities; and
 - The agency has approached Council in writing; and
 - Council is satisfied that the information is to be used by that agency for the proper and lawful function(s) of that agency; and
 - Council is satisfied that the personal information is reasonably necessary for the exercise of that agency's function(s); or
- The information 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; or
- Council is requested by a potential employer to verify:
 - That a current or former Council staff member works, or has worked, for Council;
 - The duration of the employment with Council;
 - The position(s) undertaken by the employee during any period of employment.
- The Privacy Code provisions do not permit, or authorise, Council to provide any information or opinion as to a person's suitability for a particular position, or about their performance or conduct during any

period of service. Such personal information may only be provided to third parties with the express consent of the individual concerned.

Exemptions for HPP 11:

Non-compliance is permitted under the following circumstances:

- Council is lawfully authorised or required to not comply;
- Non-compliance is permitted, necessarily implied or reasonably contemplated under an Act or any other law;
- The use is for the purpose of a disclosure by Council to another public sector agency under the administration of the Minister for Local Government (for example, the Office of Local Government) or a public sector agency under the administration of the Premier for the purpose of informing the Minister (or Premier) about any matter within the Minister's (or Premier's) administration (HPP 10(4)); or
- The use is necessary for the purpose of Council investigating or handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred to Council from or made by an investigative agency as per HPP 10(6)

10. SPECIAL RESTRICTIONS ON DISCLOSURE OF PERSONAL INFORMATION (IPP 12)

Council will not disclose personal information that relates to an individual's ethnicity/racial origin, political opinions, religion or philosophical beliefs, trade union membership, 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.

Council will not disclose personal information outlined above to any person or body who is in a jurisdiction outside New South Wales or to the Commonwealth unless such transborder disclosure is permitted under section 13 of this Part.

Exemptions for IPP 12:

Non-compliance with IPP 12 is permitted where:

- Section 27A of the PPIP Act – where the disclosure is for the purpose of providing the information to another public sector agency or the disclosure to Council is from another public sector agency; and
 - The disclosure is reasonably necessary for Council to deal with, or respond to correspondence from a Minister or member of Parliament; or
 - To enable inquiries to be referred between Council and other public sector agencies; or
 - To enable the auditing of the accounts or performance of Council
- Section 27B of the PPIP Act – where the disclosure of the information is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest; and
 - The research purpose cannot be served by disclosing information that does not identify the individual, or from disclosing information from which the individual's identity cannot be reasonably ascertained, and it is impractical for Council to seek the consent of the individual for the disclosure of the information; or
 - Reasonable steps are taken to de-identify the information before disclosure, and (where the information could reasonably be expected to identify individuals) the information is not published in a publicly available publication; or
 - The disclosure of information mentioned above must always be in accordance with guidelines, if any, issued by the Privacy Commissioner.
- Section 28(3) of the PPIP Act where the disclosure is:
 - By Council to another public sector agency (or vice versa) under the administration of the same Minister and the purpose is that of informing that Minister about any matter within the administration; or

- By another public sector agency to Council (or vice versa) under the administration of the Premier if the disclosure is for the purpose of informing the Premier about any matter.

11. IDENTIFIERS (HPP 12)

Council will only attribute an identification number to health information if it is reasonably necessary for Council to carry out its functions effectively.

12. ANONYMITY (HPP 13)

Wherever it is lawful and practicable, Council will provide individuals the opportunity to not identify themselves when entering into health information related transactions with Council or when receiving health services from Council (if any).

13. TRANSBORDER DATA FLOWS AND DATA FLOW TO COMMONWEALTH AGENCIES (IPP 12, HPP 14)

Council will not transfer personal or health information to any person or body outside NSW or to a Commonwealth agency unless:

- The transborder transfer of information is first permitted under a section of this Plan; and
- The transfer is in accordance with the Information and Privacy Commission's factsheet Guidance: transborder disclosure principle; and
- Transborder consent has been expressly given by the individual(s) concerned for the transfer of information from Council to another jurisdiction; or
- It is necessary for the performance execution or conclusion of a contract between the person concerned and Council, or in the interest of the person between Council and a third person; or
- All of the following apply:
 - It is for the benefit of the person concerned; and
 - It is impracticable to obtain the consent of the person to that transfer; and

- If consent could be obtained, the person would likely give it; or
- It is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of an individual or other person; or a serious threat to public health, or safety; or
- The transfer is authorised, permitted or required under an Act or any other law; or
- Council is satisfied that the recipient of the information is subject to a law, binding scheme or contract that upholds principles that are consistent with the HPPs; and
- Council has taken reasonable steps to ensure that the information will not be held, used, or disclosed by the recipient in any manner that is inconsistent with the HPPs.

Exemptions to IPP 12:

Non-compliance with IPP 12 is permitted:

- Section 23(6A) of the PPIP Act where:
 - Council is providing the information to another public sector agency or is receiving information from another public sector agency; and
 - The disclosure is reasonably necessary for law enforcement purposes.
- Section 23(7) of the PPIP Act where the disclosure of the information concerned is reasonably necessary for the purpose of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed.
- Section 25 of the PPIP Act where non-compliance by Council is lawfully authorised, required, permitted, necessarily implied or reasonably contemplated under an Act or any other law;
- Section 26(2) of the PPIP Act if the individual to whom the information relates has expressly consented to Council not complying with IPP 12
- Section 27A of the PPIP Act – where the disclosure is for the purposes of providing the information to another public sector agency or the disclosure to Council is from

another public sector agency; and

- The disclosure is reasonably necessary for Council to deal with, or respond to correspondence from a Minister or member of Parliament; or
 - To enable inquiries to be referred between Council and other public sector agencies; or
 - To enable the auditing of the accounts or performance of Council.
- Section 27B of the PPIP Act – where the disclosure of the information is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest; and
 - The research purpose cannot be served by disclosing information that does not identify the individual, or from disclosing information from which the individual's identity cannot be reasonably ascertained, and it is impractical for Council to seek the consent of the individual for the disclosure of the information; or
 - Reasonable steps are taken to de-identify the information before disclosure, and (where the information could reasonably be expected to identify individuals) the information is not published in a publicly available publication; or
 - The disclosure of information under the above clauses must always be in accordance with guidelines, if any, issued by the Privacy Commissioner.

Section 28(3) of the PPIP Act where the disclosure is:

- By Council to another public sector agency (or vice versa) under the administration of the same Minister and the purpose is that of informing that Minister about any matter within the administration; or
- By another public sector agency to Council (or vice versa) under the administration of the Premier if the disclosure is for the purpose of informing the Premier about any matter.

14. AUTHORISED

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.

IMPLEMENTATION OF THE PLAN

Training – Council staff (including employees, contractors, consultants and councillors)

Council staff receive training and information in relation to this Plan and their individual obligations and responsibilities under the PPIP Act and the HRIP Act as part of the induction to Council and whenever any changes to legislation or this Plan requires additional training.

Employees are also provided with specific information regarding what, if any, personal or health information is held by Council in relation to them and storage of such information on electronic and/or paper-based files.

Council staff who require assistance with the understanding and/or application of this Plan, the PPIP Act, the HRIP Act, the Privacy Code and/or related legislation may seek assistance by contacting the Public Information Officer or the Manager Human Resources.

Distribution of Information

This Plan and Council's Privacy Statement and related policies and procedures are distributed to Council staff via:

- Council's intranet site;
- Council's Website;
- Reliansys and Promapp Governance Software Programs; and
- Council's electronic content management system – Content Manager.

This Plan, Council's Privacy Statement and related policies are distributed to the community via:

- Council's website
- In person at Council's Administration Centres
- Through a request for information via council@wentworth.nsw.gov.au

Confidentiality

The obligation of confidentiality is additional to, and separate from, that of privacy. A duty to withhold information lies at the heart of both concepts. An obligation of confidentiality exists for all Council staff, whether express or implied as a matter of law.

Information that may be confidential is also likely to have a separate, independent obligation attached to it in the form of privacy and, in that regard, a release will be required. In the case of privacy, the person to whom the information relates is required to provide the release.

Prevention of misuse of information

Council has implemented a wide range of measures designed to prevent and protect personal or health information from misuse through inappropriate or unlawful collection, access, use, storage, disclosure or destruction.

These steps include (but are not limited to):

- Restriction of access to information to authorised individuals. Restriction includes strict limitations on who may access, alter, amend, update, create, store or disclose

records held by Council. Limitations are enforced through a variety of mechanisms including informal delegations, restricted access to systems and physical barriers to information (secure storage);

- Full audit history recorded for all electronic and digital files that detail when a record was created, accessed, amended, transferred, updated or destroyed and by whom;
- Regular internal and external audits of information management systems and processes with oversight by Council's Audit, Risk and Improvement Committee;
- Ongoing training of staff in relation to their responsibilities and obligations in relation to information management, privacy and confidentiality;
- Implementation of policies, procedures, systems and processes designed to ensure that personal and/or health information is collected, accessed, used, stored, updated, disclosed and/or destroyed appropriately;
- Implementation of policies, procedures and processes designed to initiate prompt and appropriate action in relation to any known or suspected misuse of personal or health information collected by Council; and
- Implementation of specific security measures (for example firewalls, encryption, password protection, secure offsite storage and security access passes) designed to mitigate any risk of misuse of information held by Council.

Staff found to have engaged in any behaviour or conduct involving the misuse of personal or health information may be subject to disciplinary action up to and including termination of employment.

Penalties for misuse of personal or health information

Under section 664 of the LG Act, it is an offence for anyone to disclose information except in accordance with the provisions of that section.

Whether or not a particular disclosure is made with lawful excuse is a matter that requires legal opinion from case to case.

Penalties for misuse of information also exist under the PPIP Act and the HRIP Act as follows:

- Section 62(1) of the PPIP Act and section 68(1) of the HRIP Act – under which corrupt disclosure and use of personal information may attract a maximum penalty of 100 penalty units or imprisonment for 2 years or both;
- Section 62(2) of the PPIP Act and section 68(2) of the HRIP Act – under which inducing or attempting to induce a public sector official to disclose personal information may attract a maximum penalty of 100 penalty units or imprisonment for 2 years or both;
- Section 63(1) of the PPIA Act and section 69(1) of the HRIP Act – where it is an offence to offer to supply personal information and attracts a maximum penalty of 100 penalty units or 2 years imprisonment or both;
- Individuals convicted under section 62 or section 63(1) of the PPIP Act may be subject to confiscation of money or other benefit alleged to have been obtained in connection with any offence;
- Section 70(1) of the HRIP Act where it is an offence to threaten, intimidate, misrepresent, persuade or attempt to persuade an individual to refrain from requesting access to their health information, make a complaint to the Privacy Commissioner or NCAT, or not make an application under Part 5 of the PPIP Act;
- Section 70(2) where it is an offence to use threat, intimidation and false representation or require another person to provide consent in relation to health information, or to do, without consent, any act which requires consent. Maximum penalty units for such offences are 100 penalty points.

Section 308H of the *Crimes Act 1900* makes an offence any act where a person causes unauthorised access to or modification of restricted data (which includes personal and health information) held in a computer in circumstances where they know the access or modification is unauthorised and intent to cause the access or modification.

In addition to the above, any staff who fail to comply with, or act in breach of, any part or requirement of this Plan, policy, procedure or legislation may be subject to disciplinary action under the Wentworth Shire Council Code of Conduct.

CONTACT DETAILS

WENTWORTH SHIRE COUNCIL

Telephone: (03) 5027 5027

Email: council@wentworth.nsw.gov.au

Street Address:

26-28 Adelaide Street,
Wentworth NSW 2648

Postal Address:

PO BOX 81, Wentworth NSW 2648

INFORMATION AND PRIVACY COMMISSION NSW

Interpreter Service: 131 450

National Relay Service: 133 677 (If you are deaf or have a hearing or speech impairment)

Email: ipcinfo@ipc.nsw.gov.au

Telephone: 1800 472 679

Street address:

Level 15, McKell Building,
2-24 Kawsen Place,
Haymarket NSW 2000

Postal address:

GPO Box 7011, Sydney NSW 2001

NSW CIVIL AND ADMINISTRATIVE TRIBUNAL

Telephone: 1300 006 228

Interpreter Service: 13 14 50

National Relay Service: 1300 555 727

Email: aeod@ncat.nsw.gov.au

Street address:

Level 10, John Maddison Tower,
86-90 Goulburn Street,
Sydney NSW 2000

Postal address:

PO Box K1026, Haymarket NSW 1240



Privacy Management Plan

Appendices

APPENDIX 1 – STATUTORY DECLARATION FOR ACCESS UNDER SECTION 57 OF THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998 TO A PUBLIC REGISTER HELD BY COUNCIL

Statutory Declaration, *Oaths Act 1900* Eighth Schedule

I, the undersigned (name of applicant)
of (address),
in the State of New South Wales, do solemnly and sincerely declare that:-

I am(relationship (if any) to person inquired about)
I seek to know whetheris on the public register of
Wentworth Shire Council pertaining to*

The purpose for which I seek this information is.....
.....
.....

The purpose for which the information is required is to
.....

And I make this solemn declaration conscientiously believing the same to be true and by virtue of the
Oaths Act 1900.

Signature of the applicant Declared at
in the said State this day of two thousand and
before me.

.....
before me:

Justice of the Peace/Solicitor
.....

Name to be printed

* Applicant to describe the relevant public register

APPENDIX 2 – PRIVACY COMPLAINT: INTERNAL REVIEW APPLICATION FORM

This is an application for review of conduct under: (please select one)

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

1. Your full name:

2. Your postal address:

Telephone number:

Email address:

3. If the complaint is on behalf of someone else, please provide their details:

What is your relationship to this person (e.g. parent)?

Is this person capable of making the complaint by himself or herself?

- ☐ Yes ☐ No ☐ Unsure

4. What is the specific conduct you are complaining about? (see footnote for explanation of ‘conduct’)

5. Please tick which of the following describes your complaint: (you may tick more than one option)

- ☐ Collection of my personal or health information
- ☐ Security or storage of my personal or health information
- ☐ Refusal to let me access or find out about my own personal or health information
- ☐ Accuracy of my personal or health information
- ☐ Use of my personal or health information
- ☐ Disclosure of my personal or health information
- ☐ Other
- ☐ Unsure

6. When did the conduct occur (date)? (please be as specific as you can)

7. When did you become aware of this conduct (date)?

8. You need to lodge this application within six months of the date at Q.7.

If more than six months has passed, you will need to ask Council for special permission to lodge a late application. Please explain why you have taken more than six months to make your complaint (for example: I had other urgent priorities – list them, or while the conduct occurred more than six months ago, I only recently became aware of my privacy rights, etc):

9. What effect did the conduct have on you?

10. What effect might the conduct have on you in the future?

11. What would you like to see Council do about the conduct? (for example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)

I understand that this form will be used by Council to process my request for an internal review.

I understand that details of my application will be referred to the Privacy Commissioner in accordance with section 54(1) of the *Privacy and Personal Information Protection Act*; or section 21 of the *Health Records and Information Privacy Act*; and that the Privacy Commissioner will be kept advised of the progress of the internal review.

Your signature:

Date:

SEND THIS FORM TO: council@wentworth.nsw.gov.au

For more information on the PPIP Act or the HRIP Act, visit: www.ipc.nsw.gov.au

Document Approval

This document is the latest version of this document as approved by the General Manager.
All previous versions of this document are null and void.

This document may be amended or revoked by the General Manager at any time.

Signed:
General Manager Wentworth Shire Council



Wentworth Shire Council

26-28 Adelaide Street, Wentworth NSW 2648

P: 03 5027 5027 | E: council@wentworth.nsw.gov.au

wentworth.nsw.gov.au