REVISED Privacy Management Plan

PORT STEPHENS COUNCIL

council@portstephens.nsw.gov.au | 02 4988 0255
PORTSTEPHENS.NSW.GOV.AU

TABLE OF CONTENTS

PART 1 – INTRODUCTION

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

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

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

The Privacy and Personal Information Protection Act 1998 ("PPIPA") provides for the protection of personal information and for the protection of the privacy of individuals.

Section 33 of the PPIPA requires all councils to prepare a Privacy Management Plan (the "Plan") to deal with:

- the devising of policies and practices to ensure compliance by the Council with the requirements of the PPIPA and the Health Records and Information Privacy Act 2002 ("HRIPA");
- the dissemination of those policies and practices to persons within the Council;
- the procedures that the Council proposes for internal review of privacy complaints;
- such other matters as are considered relevant by the Council in relation to privacy and the protection of personal information held by it.

This Plan has been prepared for the purpose of section 33 of the PPIPA.

PPIPA provides for the protection of personal information by means of 12 Information Protection Principles. Those principles are listed below:

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

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

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

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

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

This plan should also be read in conjunction with Council's endorsed policies and implemented procedures, all of which can be accessed by clicking here.

Nothing in this Plan is to:

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

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

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

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

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

1.1 What is "personal information"?

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

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

1.2 What is not "personal information"

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

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

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

Council considers the following to be publicly available publications:

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

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

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

1.3 Application of this Plan

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

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

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

1.4 Personal Information held by Council

The Council holds personal information concerning Councillors, such as:

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

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

- rates records; and
- DA applications and objections; and
- various types of health information (see page 37 for detailed examples).

The Council holds personal information concerning its employees, such as recruitment material, leave and payroll data, personal contact information, performance management plans, disciplinary matters, pecuniary interest returns, wage and salary entitlements and health information (such medical certificates and workers compensation claims).

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

Under section 739 of the *Local Government Act 1993* ("LGA") a person can make an application to suppress certain material that is available for public inspection in circumstances where the material discloses or would disclose the person's place of living if the person considers that the disclosure would place the personal safety of the person or their family at risk.

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

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

1.6 Caution as to unsolicited information

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

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

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

PART 2 – PUBLIC REGISTERS

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

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

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

Disclosure in relation to public registers must comply with Part 6 of the PPIPA and the Privacy Code of Practice. Personal information cannot be accessed by a person about another person unless the personal information is contained in a public register. Where personal information is contained in a public register, then Part 6 of the PPIPA applies to determine whether access to that information will be given to another person.

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

The following list identifies public registers held by Council.

Act / Regulation	Section		Purpose	Contact
*Local Government Act	53	Land Register	Identify land vested in Council or under Council's control	Register can be accessed from Council's website.
	113	Record of Approvals	Identify approvals granted under the Act	Development Services.
	449-450A	Register of Pecuniary Interests	Identify pecuniary interest of Councillors and designated persons	Councillor returns are available on Council's website. For other designated persons returns please contact Council.
Environmental Planning and Assessment Act	100	Register of Consents and Approvals	Identify approvals, consents and related appeals under the Act	Some information is available from Council's website or alternately from Development Services.
	149G	Record of Building Certificates	Identify building certificates	Development Services

Act / Regulation	Section		Purpose	Contact
Protection of the Environment Operations Act	308	Public register of licences	Identify licences granted under the Act	Development Services/Governance.
Impounding Act	30 & 31	Record of Impounding	Identify impounding action by Council	Development Services/Governance.
Government Information (Public Access) Act	25	Disclosure Log of Access Applications	Identify access applications where there is a public interest and Council has determined to provide access to the information	Register can be accessed from Council's website.
	27	Register of Government Contracts	Identify Council contracts that have (or are likely to have) a value of $150,000 or more	Register can be accessed from Council's website.
Government Information (Public Access) Regulation 2009	Sch1. 1(3)(d)	Register of graffiti removal	Identify graffiti removal work	Facilities and Services
	Sch1. 1(3)(e)	Register of current political donations	Identify current political donations	Register can be accessed from a link on Council's website.
	Sch1. 1(3)(e)	Register of planning decisions	Identify voting on planning matters of the elected council	Register can be accessed from Council's website.
Local Government Act	377-378	Register of Delegations	Identify functions delegated by the General Manager to Council Officers	Register can be accessed from Council's website.
	602	**Rates Record	In relation to a parcel of land, identify: • the value • rate liability the owner or lessee	Register can be sought by informal request under the GIPA Act.

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

**Note – owner contact information will not be provided.

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

A list of other registers held by Council is available from Council's website. It should be noted that a number of these registers are not public registers. The Information Protection Principles, this Plan, any applicable Codes and the PPIPA apply to those registers or databases.

2.1 Public registers, the PPIPA and the HRIPA

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

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

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

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

Council also needs to consider the Privacy Code of Practice for Local Government which has the effect of modifying the application of Part 6 of the PPIPA (the “public register” provisions).

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

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

2.2 Effect on section 6 of the GIPA Act

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

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

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

(i) if it is allowed under section 57(1) of the PPIPA; **and**
(ii) there is no overriding public interest against disclosure of the information under section 6 of the GIPA Act.

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

2.3 Where some information in the public register has been published

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

For example, the Register of Consents and Approvals held by Council under section 100 of the Environmental Planning and Assessment Act requires Council to advertise or publish applications for development consent.

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

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

Registers should not be published on the internet.

2.4 Disclosure of personal information contained in the public registers

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

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

Secondary purpose of all Public Registers

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

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

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

Other Purposes

Persons or organisations who apply to Council to have access to the information contained in any public register for a purpose not related to the purpose of the register, may be given access at the discretion of Council but only in accordance with the Privacy Code of Practice for Local Government concerning Public Registers.

2.5 Applications for access to own records on a public register

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

2.6 Applications for suppression in relation to a public register

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

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

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

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

Any information that is removed from, or not placed on, that aspect of a public register to be made public may be kept on the register for other purposes. That is, the information may still be used for council functions, but it cannot be disclosed to other parties.

An application for suppression should be made in writing addressed to the General Manager and must outline the reasons for the request. The Council may require supporting documentation where appropriate.

PART 3 – THE INFORMATION PROTECTION PRINCIPLES

3.1 Information Protection Principle 1 – Section 8

Section 8 Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless:
(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and
(b) the collection of the information is reasonably necessary for that purpose.

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes no provision to depart from the requirements of this principle.	Council will only collect personal information for a lawful purpose as part of its proper functions. The LGA governs Council's major obligations and functions. Section 22 of the LGA provides other functions under other Acts. Some of those Acts are as follows: • Community Land Development Act 1989 • Companion Animals Act 1998** • Conveyancing Act 1919 • Environmental Planning and Assessment Act 1979 • Fire Brigades Act 1989 • Fluoridation of Public Water Supplies Act 1957 • Food Act 2003 • Impounding Act 1993 • Library Act 1939 • Protection of the Environment Operations Act 1997 • Public Health Act 2010 • Recreation Vehicles Act 1983 • Roads Act 1993 • Rural Fires Act 1997 • State Emergency Service Act 1989 • Strata Schemes Development Act 2015 • Strata Schemes Management Act 2015 • Swimming Pools Act 1992 This list is not exhaustive.

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

- Coastal Management Act 2016;
- Environmental Offences and Penalties Act 1989;
- Government Information (Public Access) Act 2009;
- Heritage Act 1977;
- State Emergency and Rescue Management Act 1989;
- Unclaimed Money Act 1995;
- Unhealthy Building Land Act 1990.

The circumstances under which Council may collect information, including personal information, are varied and numerous. Examples of circumstances in which Council may collect personal information include:

- Making, receiving or investigating a complaint
- For recruitment purposes
- Responding to or conducting surveys
- Rating information
- Processing general enquiries
- Issuing approvals or orders
- CCTV Footage

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

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

Companion Animals Act

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

Role of the Privacy Contact Officer

In order to ensure compliance with Information Protection Principle 1, internet contact forms, rates notices, application forms of whatsoever nature, or written requests by which personal information is collected by Council; will be referred to the Privacy Contact Officer prior to adoption or use. The Privacy Disclaimer at Appendix 2 is to be included on all forms and other documents where information is being solicited from individuals.

The Privacy Contact Officer will also provide advice as to:

1. Whether the personal information is collected for a lawful purpose;

2. If that lawful purpose is directly related to a function of Council; and

3. Whether or not the collection of that personal information is reasonably necessary for the specified purpose.

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

3.2 Information Protection Principle 2 – Direct Collection

Section 9 Collection of personal information directly from individual

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

(a) the individual has authorised collection of the information from someone else, or
(b) in the case of information relating to a person who is under the age of 16 years—the information has been provided by a parent or guardian of the person.

The Privacy Code of Practice for Local Government	Council Policy
The Code makes provision for Council to depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.	The compilation or referral of registers and rolls are the major means by which the Council collects personal information. For example, the information the Council receives from NSW Land Registry Services would fit within section 9(a) above. Other means include forms that customers may complete and lodge with Council for development consent, companion animal registration, applications for specific inspections or certifications or applications in respect of tree preservation orders. In relation to petitions, the Council will treat the personal information contained in petitions in accordance with PPIPA. Where Council or a Councillor requests or requires information from individuals or groups, that information will be treated in accordance with PPIPA. Council regards all information concerning its customers as information protected by PPIPA. Council will therefore collect all personal information directly from its customers except as provided in section 9 or under other statutory exemptions or Codes of Practice. Council may collect personal information from other public sector agencies in respect of specific statutory obligations where it is authorised by law to do so. Where Council anticipates that it may otherwise need to collect personal information indirectly it will first obtain the authorisation of each individual under section 9 (a) of the PPIPA.

External and related bodies

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

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

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

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

- obtain a written authorisation and consent to that collection; and
- notify those persons in accordance with Information Protection Principle 3 as to the intended recipients and other matters required by that principle.

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

Investigative Functions

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

Existing statutory exemptions under the Act

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

The relevant statutory exemptions follow:

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

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

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

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

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

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

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

Further Explanation regarding IPP 2

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

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

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

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

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

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

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

3.3 Information Protection Principle 3 - Requirements when collecting personal information

Section 10 Requirements when collecting personal information

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

(a) the fact that the information is being collected,
(b) the purposes for which the information is being collected,
(c) the intended recipients of the information,
(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,
(e) the existence of any right of access to, and correction of, the information,
(f) the name and address of the agency that is collecting the information and the agency that is to hold the information.

The Privacy Code of Practice for Local Government	Council Policy
The Code makes provision for Council to depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be, or may be, conferred upon the person to whom the information relates.	Where Council proposes to collect personal information directly from the person, it will inform that person that the personal information is being collected, what is done with that information and who the intended recipients will be. Council apply the Privacy disclaimer (see Appendix 2) to all applications to inform individuals and to meet the requirements of Information Protection Principle 3 (IPP 3). The following are examples of application procedures that will require aa Privacy disclaimer in accordance with IPP 3: • Lodging Development Applications; • Lodging objections to Development Applications; • Lodging applications for approval under the LGA; and • When collecting an impounded item. In relation to the Privacy Disclaimer that may be attached to a Development Application provided to objectors, it could be stated that objectors have a right to remain anonymous if they so choose. However, should they need to substantiate their objections, anonymous objections may be given less weight (or no weight) in the overall consideration of the Application.

Post - Collection

Where Council collects personal information indirectly from another public sector agency in respect of any one of its statutory functions, it will advise those individuals that it has collected their personal information by letter. The letter should ensure the requirements of IPP 3 are met.

A common example of the collection of information from another public sector agency is the NSW Land Registry Services. Council receives information as to new ownership changes when property is transferred from one owner to the next.

External and related bodies

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

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

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

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

Investigative Functions

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

Existing statutory exemptions under the Act

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

The relevant statutory exemptions follow:

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

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

(i) investigating or otherwise handling a complaint or other matter that could be referred or made to, or has been referred from or made by, an investigative agency; and
(ii) if compliance might detrimentally affect (or prevent the exercise of) the Council's complaint handling or investigative functions.

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

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

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

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

Disclosure of information of research purposes

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

3.4 Information Protection Principle 4 - Other requirements relating to collection of personal information

Section 11 Other requirements relating to collection of personal information

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

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

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes no provision to depart from this principle.	Council will seek to ensure that no personal information is collected which is not directly relevant to its proper functions. Council collects personal information through the various forms that customers may complete and lodge with Council. Before adoption of a new form, a draft form will be reviewed for compliance with Information Protection Principle 4 by the EEO Officer, Council's solicitor, Public Officer or other suitable person. Should Council have any residual doubts, the opinion of the Office of the Privacy Commissioner NSW will be sought.

3.5 Information Protection Principle 5 - Retention and security of personal information

Section 12 Retention and security of personal information

A public sector agency that holds personal information must ensure:

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

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

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

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes no provision to depart from this principle.	Council may comply with this principle by using any or all of the following or similar documents: • Council's ICT Systems Access and Cyber Security Management Directive. This document defines the minimum requirements for controlling access to Council's systems and information to ensure appropriate access to systems can be provided whilst adequate protection from exposure to cyber threats is provided.

<u>Disclosure of information of research purposes</u>

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

3.6 Information Protection Principle 6 - Information held by agencies

Section 13 Information about personal information held by agencies

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

(a) whether the agency holds personal information, and

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

(c) if the agency holds personal information relating to that person:
(i) the nature of that information, and
(ii) the main purposes for which the information is used, and
(iii) that person's entitlement to gain access to the information.

The Privacy Code of Practice for Local Government	Council Policy
The Code makes no provision to depart from this principle.	Section 13 of the PPIPA requires a council to take reasonable steps to enable a person to determine whether the council holds personal information about them. If Council holds any information about a person, upon request it will advise them the nature of that information, the main purposes for which it is held, and that person's entitlement to access. As a matter of practicality, not every item of personal information, however insignificant, will be capable of ascertainment. Under section 20(5) of the PPIPA, Information Protection Principle 6 is subject to any applicable conditions or limitations contained in the Government Information (Public Access) Act 2009 ("GIPA Act"). Council must consider the relevant provisions of the GIPA Act. Where Council receives an application or request by a person as to whether council holds information about them, Council will undertake a search of its records to answer the enquiry. Council may ask the applicant to describe what dealings the applicant has had with council in order to assist Council to conduct the search. Council will ordinarily provide a response to applications of this kind within 20 working days of the application being made. The fee structure is commensurate to that of the Council's GIPA Act rates structure.

Investigative Functions

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

Existing exemptions under the Act

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

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

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

Reporting matters

Council's Agency Information Guide (AIG) provides details on the type of information that is collected by Council. The AIG is available from Council's website.

Further information

Further details concerning how to apply to Council for this information can be addressed in writing to:

The Privacy Officer
PO BOX 42
Raymond Terrace NSW 2324

Or by email: council@portstephens.nsw.gov.au

3.7 Information Protection Principle 7 - Access to personal information held by agencies

Section 14 Access to personal information held by agencies

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes no provision to depart from this principle.	Section 14 of the PPIPA requires a council, at the request of any person, to give access to that person to personal information held about them. Compliance with Information Protection Principle 7 does not allow disclosure of information about other people. If access to information that relates to someone else is sought, the application must be made under the GIPA Act, unless Information Protection Principles 11 and 12 or the Public Register provisions apply. Where a person makes an application for access under the PPIPA and it is involved or complex, it may be referred, with the written consent of the applicant, as an application under the GIPA Act. However, use of the GIPA Act is to be a last resort. The applicant has the right to insist on being dealt with under PPIPA. Under section 20(5) of the PPIPA, Information Protection Principle 7 is subject to any applicable conditions or limitations contained in the Government Information (Public Access) Act 2009 ("GIPA Act"). Council must consider the relevant provisions of the GIPA Act. Customers wishing to exercise their right of access to their own personal information should apply in writing or direct their enquiries to the General Manager, who will make a determination. This can also be undertaken under the GIPA Act through an informal request. Members of staff wishing to exercise their right of access to their personal information should apply in writing on the attached form or direct their inquiries to the HR Manager, who will deal with the application. In order to comply with the requirement to provide the requested information "without excessive delay or expense", Council will ordinarily provide a response to applications of this kind within 20 working days of the application being made.

Investigative Functions

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

Existing exemptions under the Act

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

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

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

3.8 Information Protection Principle 8 - Alteration of personal information

Section 15 Alteration of personal information

(1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:
(a) is accurate, and
(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

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

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

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

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

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes no provision to depart from this principle.	Section 15 of the PPIPA allows a person to make an application to council to amend (this includes by way of corrections, deletions or additions) personal information held about them so as to ensure the information is accurate, and, having regard to the purpose for which the information is collected, relevant to that purpose, up to date and not misleading. Council wishes to have its information current, accurate and complete. Proposed amendments or changes to the personal information held by the Council are welcomed. If Council declines to amend personal information as

	requested, it will on request of the individual concerned, place an addendum on the information in accordance with section 15(2) of the PPIPA. Where there are complaints that are or could be the subject of a staff complaint or grievance, they will be referred to the HR Manager in the first instance and treated in accordance with the "Grievance and Complaint Handling Procedures". Any alterations that are or could be the subject of a customer complaint or grievance will be referred to the General Manager, who will make a determination in relation to the matter.

Investigative Functions

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

Existing exemptions under the Act

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

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

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

Procedure

Where information is requested to be amended (either by way of correction, deletion or addition), the individual to whom the information relates, must make a request, in writing to Council's Privacy Officer. That request should be accompanied by appropriate evidence as to the cogency of the making of the amendment, sufficient to satisfy the Council that the proposed amendment is factually correct and appropriate. The Council may require further documentary evidence to support certain amendments. Council will not charge to process an application to amend a record under s.15.

Where Council is not prepared to amend

If the Council is not prepared to amend the personal information in accordance with a request by the individual the Council may attach to the information in such a manner

as is capable of being read with the information, any statement provided by that individual.

Where an amendment is made

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

State Records Act

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

How to apply

If an alteration is requested, Council would require this request to be made in writing and addressed to:

The Privacy Officer
PO BOX 42
Raymond Terrace NSW 2324

Or by email: council@portstephens.nsw.gov.au

3.9 Information Protection Principle 9 - Agency must check accuracy of personal information before use

Section 16 Agency must check accuracy of personal information before use

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes no provision to depart from this principle.	The steps taken to comply with section 16 will depend on the age of the information, its likelihood of change and the particular function for which the information was collected. The more significant the information, the greater the necessity that checks to ensure its accuracy and currency be undertaken prior to its use. This however does not detract from the obligation on Council to take such steps as are reasonable to ensure that any personal information being used is accurate before using it. For example, each employee's record should be updated when there is any change of circumstances or when the employee's contact details change.

3.10 Information Protection Principle 10 - Limits on use of personal information

Section 17 Limits on use of personal information

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

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

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

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes provision that Council may use personal information for a purpose other than the purpose for which it was created in the following circumstances: (i) where the use is in pursuance of Council's lawful and proper function/s and Council is satisfied that the personal information is reasonably necessary for the exercise of such function/s; or (ii) where personal information is to be used for the purpose of conferring upon a particular person, an award, prize, benefit or similar form of personal recognition.	Council will seek to ensure that information collected for one purpose will be used for that same purpose. Where Council may need to use personal information collected for one purpose for another purpose, it will first gain the consent of the individual concerned, unless an exemption applies.

Explanatory Note

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

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

External and related bodies

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

- Council employees
- Council owned businesses
- Council consultants;
- Private contractors; and
- Council committees.

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

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

The form of consent should include the following elements:

I, (1) .....

of (2) .....

hereby consent under section 17(a) of the Privacy and Personal Information Protection Act 1998 to (3): .....

.....

using the information collected from me by (4): .....

.....

for the purpose of (5): .....

.....

Signature .....

Name to be printed .....

Date signed / /

(1) insert full name

(2) insert address

(3) insert Council name

(4) insert name of collecting body/person

(5) insert purpose/s info was collected for

Investigative Functions

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

Existing exemptions under the Act

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

Section 23(4) of the PPIPA permits Council not to comply with Information Protection Principle 10 where the use of the information for another purpose is reasonably necessary for law enforcement purposes or for the protection of the public revenue. Law enforcement purposes means a breach of the criminal law and criminal law enforcement. This section does not remove the rights of an accused person. Protection of the public revenue means a fraud with respect to taxes or other revenue earning processes such as avoidance of stamp duty.

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

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

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

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

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

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

3.11 Information Protection Principle 11 - Limits on disclosure of personal information

Section 18 Limits on disclosure of personal information

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

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

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

(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes provision for council to depart from this principle in the circumstances described below: 1. Council may disclose personal information to public sector agencies or public utilities on condition that: (i) the agency or utility provider has approached Council in writing; (ii) Council is satisfied that the information is to be used by that agency for the proper and lawful function/s of that agency or utility provider, and	Council will not disclose the information to another person or other body, unless the disclosure is directly related to the purpose for which the information was collected or where the Council has no reason to believe that the individual concerned would object to the disclosure. Council may disclose personal information to another person or other body where this disclosure is directly related to the purpose for which the personal information was collected and the individual concerned is reasonably likely to have been aware, (or has been made aware in accordance with section 10), of the intended recipients of that information. “Directly related” can mean the disclosure to another person or agency to deliver a service which supplements that of Council or disclosure to a consultant for the purpose of assessing or reviewing the delivery of a program to which the original collection relates. The Ccouncil may disclose personal information to another person or other body where this disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or

(iii) Council is satisfied that the personal information is reasonably necessary for the exercise of that agency or utility provider's function/s. 2. Where personal information which has been collected about an individual is to be disclosed for the purpose of conferring upon that person, an award, prize, benefit or similar form of personal recognition. 3. Where Council is requested by a potential employer, it may verify that a current or former employee works or has worked for Council, the duration of that work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.	another person.

Public Registers

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

Investigative Functions

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

Existing exemptions under the Act

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

Section 23(5)(a) of the PPIPA permits non-compliance with Information Protection Principle 11 where disclosure is made to a law enforcement agency in connection with proceedings for an offence or for law enforcement purposes. *Law enforcement purposes* means a breach of the criminal law and criminal law enforcement. However Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

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

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

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

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

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

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

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

(Note: “investigative agency” is defined at s.3 of PPIPA.)

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

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

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

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

Suppression

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

3.12 Information Protection Principle 12 - Special restrictions on disclosure of personal information

Section 19 Special restrictions on disclosure of personal information

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

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

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

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

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

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

(5) Subsection (2) does not apply:

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

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

The Privacy Code of Practice for Local Government	Council Policy
The Code makes provision for Council to depart from this principle in the circumstances described below: 1. For the purposes of s.19(2) only, where Council is requested by a potential employer outside New South Wales, it may verify that a current or former employee works or has worked for Council, the duration of that	Council will not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.	

Public Registers

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

Investigative Functions

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

Existing exemptions under the Act

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

Section 23(7) of the PPIPA permits non-compliance with Information Protection Principle 12 where the disclosure is necessary to investigate an offence or where there are reasonable grounds to believe an offence has been or may be committed.

Section 25(a) of the PPIPA permits non-compliance with Information Protection Principle 12 where Council is lawfully authorised or required not to comply with the principle.

Section 25(b) of the PPIPA permits non-compliance with Information Protection Principle 12 where non-compliance is “necessarily implied” or “reasonably contemplated” under any Act or law.

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

Section 28(2) permits non-compliance with Information Protection Principle 12 where, in the case of health information, the consent of the person cannot reasonably be obtained and the disclosure is made by an authorised person to another authorised person. “Authorised person” means a medical practitioner, health worker, or other official or employee providing health or community services who is employed or engaged by a public sector agency.

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

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

Suppression

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

PART 4 – HEALTH PRIVACY PRINCIPLES

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

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

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

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

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

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

- Some councils run Podiatry services;
- Information may be collected through a healthy community program;
- Children's immunization records; and
- Family counsellor/youth support workers records.

HPPs 1-4 concern the collection of health information, HPP 5 concerns the storage of health information, HPPs 6-9 concern the access and accuracy of health information, HPP 10 concerns the use of health information, HPP 11 concerns the disclosure of health information, HPPs 12-13 concern the identifiers and anonymity of the persons to which health information relate, HPPs 14-15 concern the transferral of health information and the linkage to health records across more than one organisation.

Health Privacy Principle 1

Purposes of collection of health information

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

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and
(b) the collection of the information is reasonably necessary for that purpose.

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

Health Privacy Principle 2

Information must be relevant, not excessive, accurate and not intrusive

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

(a) the information is collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and
(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Council complies with this Health Privacy Principle by collecting only the information that is deemed to be necessary to carry out the function to which the collection relates. This is implemented by control measures such as directed questions on forms to ensure the required extent of disclosure is obtained.

Prior to using personal information, Council may take reasonable steps to check its accuracy by taking the following into consideration:

- What was the purpose for which the information was collected?
- When was it collected?
- What was the contact in which the information was collected?
- What purpose is the information going to be used for?
- Who has access to this information? In addition to this, who has access to edit it?

- How important is the accurary of this information?
- What is the possible impact on the individual if the information is inaccurate, out of date or irrelevant?
- Is it possible to correct inaccuracies prior to use?
- What are the barriers to checking the information? I.e. cost or resources

Health Privacy Principle 3

Collection to be from the individual concerned

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

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

Some examples of when health information is collected may include:

- When an incident concerning public liability has occurred and an injury has been alleged or sustained. In order to advise Council's insurers of the incident and potential or impending claim, Council may require the provision of health information to demonstrate the extent of injury.
- Workers compensation claims
- Accessing leave entitlements including sick leave
- Mandatory testing including for recruitment purposes

Health Privacy Principle 4

Individual to be made aware of certain matters

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

(a) the identity of the organisation and how to contact it,
(b) the fact that the individual is able to request access to the information,
(c) the purposes for which the information is collected,
(d) the persons to whom (or the type of persons to whom) the organisation usually discloses information of that kind,
(e) any law that requires the particular information to be collected,
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

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

(a) making the individual aware of the matters would impose a serious threat to the life or health of any individual, or
(b) the collection is made in accordance with guidelines issued under subclause (3).

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

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

(a) the individual to whom the information relates has expressly consented to the organisation not complying with it or,
(b) the organisation is lawfully authorised or required not to comply with it, or
(c) non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under any Act or any other law including the State Records Act 1998), or
(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or
(e) the information concerned is collected for law enforcement purposes or,
(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

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

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

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

Council Policy

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

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

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

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

If Council collects health information about a person from someone else, Council will take reasonable steps to ensure that the subject of the information is aware of the above points (HPP 4).

Council complies with this HPP by collecting only the information that is deemed to be necessary to carry out the function to which the collection relates. This is implemented by control measures such as directed questions on forms to ensure the required extent of disclosure is obtained.

When health information is collected, notification of the collection can be found on the relevant form requesting the information. When health information is not provided via written mechanisms the third party is advised of this collection verbally.

Health Privacy Principle 5

Retention and Security

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

(a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
(b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and

(c) the information is protected, by taking such security safeguards as are reasonable in the circumstances against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and
(d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of an organisation is done to prevent the unauthorised use or disclosure of the information.

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

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

(a) the organisation is lawfully authorised or required not to comply with it, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

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

Council Policy

Council will store health information securely and protect health information from unauthorised access, use or disclosure. Health information will not be kept for any longer than is necessary and will be disposed of appropriately (HPP 5).
Council may comply with this principle (HPP 5) by using any or all of the following or similar documents:

- Council's ICT Systems Access and Cyber Security Management Directive. This document defines the minimum requirements for controlling access to Council's systems and information to ensure appropriate access to systems can be provided whilst adequate protection from exposure to cyber threats is provided.

Health Privacy Principle 6

Information about health information held by organisations

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable, to enable any individual to ascertain:
(a) whether the organisation holds health information, and
(b) whether the organisation holds health information relating to that individual, and
(c) if the organisation holds health information relating to that individual:
(i) the nature of that information
(ii) the main purposes for which the information is used, and
(iii) that person's entitlement to request access to the information.

(2) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

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

Health Privacy Principle 7

Access to health information

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

(2) Such requests can be made in writing and forwarded to:
The Privacy Officer
PO BOX 42
Raymond Terrace NSW 2324
Or by email: council@portstephens.nsw.gov.au

Note. Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Access to health information held by public sector agencies may also be available under the Government Information (Public Access) Act 2009 or the State Records Act 1998.

(3) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

Health Privacy Principle 8

Amendment of health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information:
(a) is accurate, and
(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to day, complete and not misleading.

(2) Such requests can be made in writing and forwarded to:
The Privacy Officer
PO BOX 42
Raymond Terrace NSW 2324
Or by email: council@portstephens.nsw.gov.au

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

individual of the amendment sought.

(4) If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.
Note. Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.
Amendment of health information held by public sector agencies may also be able to be sought under the Privacy and Personal Information Protection Act 1998.

(5) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

Health Privacy Principle 9

Accuracy

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

Council Policy
Council will provide details about what health information Council is holding about an individual and with information about why Council is storing that information and what rights of access the individual has (HPP 6). Council will allow the individual to access his or her health information without reasonable delay or expense. A request to access information can be made in writing to Council (HPP 7). Council will allow the individual to update, correct or amend his or her health information where necessary. A request to amend information can be made in writing to Council (HPP 8). Council will make sure that the health information is relevant and accurate before using it, from the information available to Council to assess the accuracy (HPP 9).

Prior to using personal information, Council may take reasonable steps to check its accuracy by taking the following into consideration:

- What as the purpose for which the information was collected?

- When was it collected?
- What was the context in which this information was collected?
- What purpose is the information going to be used for?
- Who has access to this information? And who has access to edit this information?
- How important is the accuracy of this information?
- What is the impact on the individual if the information is inaccurate, out of date or irrelevant?
- Is it possible to correct inaccuracies prior to use?
- What are the barriers to checking the information?

Health Privacy Principle 10

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

(a) **Consent**

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

(b) **Direct relation**

the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose or,

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

(c) **Serious threat to health or welfare**

the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

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

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

(d) **Management of health services**

the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

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

(B) reasonable steps are taken to de-identify the information, and

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

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

(e) **Training**
the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:
(i) either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**
the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:
(i) either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purpose of this paragraph, or

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

(h) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**
the organisation:
(i) has reasonable grounds to suspect that:
(A) unlawful activity has been or may be engaged in, or
(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a the Health Practitioner Regulation National Law (NSW), or
(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and
(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

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

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

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

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

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

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

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:
(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or
(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

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

Council Policy

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

Council takes reasonable steps to ensure that personal and health information is only accessible by the staff who require access to it in order to carry out their functions. Information collected by Council may be used by departments and units of Council that did not undertake the initial collection of the information only if the use of it is for the same purpose in which it was originally collected.

For example, if Council held information concerning a health condition relating to a member of staff and an incident occurred which caused threat to the health of the employee, the information may be relayed to an emergency services officer attending the scene. This would be only be permissible as the secondary purpose is directly related to the primary purpose the information was collected.

Health Privacy Principle 11

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

(a) **Consent**

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

(b) **Direct relation**

the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or

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

(c) **Serious threat to health or welfare**

the disclosure of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

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

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

(d) **Management of health services**

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

(i) either:

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

(B) reasonable steps are taken to de-identify the information, and

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

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

(e) **Training**

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

(i) either:

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

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify the individual, the information is not made publicly available, and
(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**

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

(i) either:

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

(B) reasonable steps are taken to de-identify the information, and

(ii) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained, and
(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Compassionate reasons**

the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:
(i) the disclosure is limited to the extent reasonable for those compassionate reasons, and
(ii) the individual is incapable of giving consent to the disclosure of the information, and
(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and
(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information, or

(h) **Finding missing person**

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

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

the organisation:
(i) has reasonable grounds to suspect that:
(A) unlawful activity has been or may be engaged in, or
(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a the Health Practitioner Regulation National Law (NSW), or
(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and
(ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) **Law enforcement**

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

(k) **Investigative agencies**

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

(l) **Prescribed circumstances**

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

(2) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or
(c) the organisation is an investigative agency disclosing information to another investigative agency.

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

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:
   (a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or
   (b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

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

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

Council Policy

Council will only disclose health information under the following circumstances:

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

Health Privacy Principle 12

Identifiers

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

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

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

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

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

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

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

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

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

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

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

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

Health Privacy Principle 13

Anonymity

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

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

An example of when an individual may request to remain anonymous may be when they are lodging a complaint about a companion animal, submissions on a development application or notification to Council of a pothole requiring repair.

An individual can request to remain anonymous verbally or in writing, depending upon how the communication is received (via email or over the phone). If an individual does elect to remain anonymous, future contact regarding the matter may not be possible or they may not be able to be updated on the outcome of the matter.

Health Privacy Principle 14

Transborder data flows and data flow to Commonwealth agencies.

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

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

(b) the individual consents to the transfer, or

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

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

(e) all of the following apply:
(i) the transfer is for the benefit of the individual,
(ii) it is impracticable to obtain the consent of the individual to that transfer,
(iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:
(i) a serious and imminent threat to the life, health or safety of the individual or another person, or
(ii) a serious threat to public health or public safety, or

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

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

In addition to the normal disclosure rules, Council will not disclose (or transfer) personal or health information to any person or body outside NSW or to a Commonwealth agency (transborder disclosure) unless one of the following exemptions apply:

- the other party is subject to a law, scheme or contract that upholds principles substantially similar to the information privacy principles
- the individual concerned has consented
- the transfer is necessary for the performance of a contract between the individual and Council or a third party • the transfer will benefit the individual concerned, but it is impracticable to obtain their consent, and if notified would likely consent
- the disclosure is reasonably believed by Council to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person
- Council has taken reasonable steps to ensure the information won't be dealt with inconsistently with the information privacy principles (e.g. we have bound the recipient by contract to privacy obligations equivalent to the principles), or
- if it is permitted by any other exemption in the Privacy legislation, permitted or required by any Act or any other law Where information is disclosed transborder,

Council will make an assessment to determine that the privacy protections operating in the destination jurisdiction are substantially similar to those in NSW and put in place contractual terms to ensure the protection of the information provided.

Where it is necessary for personal or health information to be disclosed to a third party provider, for the purposes of providing a service, Council ensures that appropriate contractual protections are included in the contract with the provider to prevent unauthorised use or disclosure of personal or health information. Contracts with third party providers include appropriate standards for data protection and require compliance with the relevant privacy principles. Where Council intends to disclose personal or health information to a third party service provider outside of NSW or to a Commonwealth agency, Council takes reasonable steps to ensure that the information it has disclosed will not be held, used or disclosed by the recipient inconsistently with the IPPs / HPPs. This is achieved by

- including contractual protections requiring the recipient to comply with the IPPs / HPPs and the Privacy Commissioner's guidance on transborder disclosures;
- making an assessment to determine that the privacy protections operating in the destination jurisdiction are substantially similar to those in NSW; and
- conducting audits over the service providers' IT systems before the contract is entered into and during the term of the contract.

Council Policy

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

Health Privacy Principle 15

Linkage of health records

(1) An organisation must not:
(a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or
(b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or
(c) the inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

(3) In this clause:

health record means an ongoing record of health care for an individual.
health records linkage system means a computerised system that is designed to link health records for an individual held by different organisations

for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

As of the date of this Plans endorsement, Council does not maintain a health records linkage system.

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

PART 5 – IMPLEMENTATION OF THE PRIVACY MANAGEMENT PLAN

5.1 Training Seminars/Induction

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

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

All new employees are required to complete on line privacy training as part of their probation period and also attend privacy training at the induction. Ongoing privacy training is provided to those employees who are responsible for handling personal information.

5.2 Responsibilities of the Privacy Contact Officer

The Public Officer within Council is responsible for the role of the Privacy Contact Officer.

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

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

- fast screen savers;
- face the computers away from the public; or
- only allow the record system to show one record at a time.

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

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

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

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

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

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

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

5.3 Distribution of information to the public

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

PART 6 – DATA BREACHES

6.1 What is a data breach?

The Mandatory Notification of Data Breach Scheme ('MNDB Scheme') is a mandatory notification requirement under the *Privacy and Personal Information Protection Act 1998* for NSW public sector agencies in the event of an 'eligible data breach'. An 'eligible data breach' occurs when there is:

- unauthorised access to, or unauthorised disclosure of, personal information held by an agency that would be likely to result in serious harm to an individual to whom the information relates
- the loss of personal information held by an agency in circumstances where unauthorised access or disclosure is likely to occur and which would be likely to result in serious harm to an individual to whom the information relates.

6.2 What is unauthorised access and unauthorised disclosure?

Unauthorised access to personal information can occur when someone accesses information without permission. For example:

- a cyber attack on a database containing personal information, or
- an agency employee intentionally opens an electronic or paper file containing personal information when they do not have permission to access that information.

Unauthorised disclosure of personal information can occur if information is provided to or accessible by people outside the agency. This could be the result of:

- simple human or technical errors without malicious intent, for example where an agency accidentally publishes a data set containing personal information on its website
- a third party downloading data from an unsecured computer system or platform
- emails containing personal information being sent to the wrong person.

Personal information held by an agency can also be accidentally lost (including where it is stolen) in circumstances where it is likely to result in unauthorised access to or disclosure of that information. For example:

- a file containing personal information is accidently left in a public place
- a laptop containing the personal information of an agency's clients is stolen from the agency's office.

6.3 What are the potential impacts of a data breach?

- Financial loss through fraud
- A likely risk of physical or psychological harm, such as by an abusive ex-partner
- Identity theft, which can affect your finances and/or credit record
- Serious harm to an individual's or Council's reputation.

6.4 Who decides if you've suffered serious harm?

Whether the unauthorised access, disclosure or loss of your personal information is likely to result in serious harm to you, will be assessed by the agency as part of its response to the data breach. This requires an objective assessment determined from the viewpoint of a reasonable person.

An agency will consider the circumstances of the breach, how likely it is that the breach will cause harm, and the consequences and severity of that harm. In making this determination, the agency may consider the following:

- the types of personal information involved, for example, an email address is likely to be considered less likely to result in serious harm than credit card details
- the sensitivity of the personal information, for example, if it relates to a person's finances, health, or sexual orientation
- whether the personal information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused
- who has access to the personal information
- whether the person/s who accessed the personal information may have a malicious intent and whether they may be able to circumvent security measures
- the nature of the likely harm
- any other matter specified in the Privacy Commissioner's guidelines.

6.5 Your right to be notified of a breach of your personal information

When a data breach occurs, Council must immediately make all reasonable efforts to contain the breach and try to reduce the likelihood that an individual will experience serious harm.

Council then has 30 days from the date they become aware of a possible data breach to assess whether that data breach is likely to result in serious harm. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

If an agency decides there has been an eligible data breach in relation to your personal information, it must notify you as soon as practicable about that breach. This means that an agency must notify you in writing and provide you with information about the eligible data breach, including:

- actions the agency has taken or plans to take to control or mitigate the harm done to you
- steps you should consider taking following an eligible data breach
- information about how to seek an internal review of the agency's conduct or make a privacy complaint to the Privacy Commissioner.

If the agency is unable to notify you directly it must publish a notification on its website and take reasonable steps to publicise the notification. The notification must remain on the agency's public notification register for at least 12 months. There are certain exemptions to the requirement that agencies notify affected individuals of a data breach. For example, if an agency acts quickly to mitigate a data breach, and because of this action the data breach is not likely to result in serious harm, there is no requirement to notify any affected individuals.

6.6 What do I do if I become aware of a suspected data breach?

If you suspect a data breach has occurred, you must immediately submit an incident form via our website. You may alternatively call Council and ask to speak with a member from our Governance team.

6.7 Where can I go to get more information about the scheme and how Port Stephens Council manage it?

- The Information and Privacy Commission publishes helpful information which can be found here: https://www.ipc.nsw.gov.au/privacy/MNDB-scheme
- Council's Data Breach page on our website
- Council's Agency Information Guide
- Council's Data Breach Policy.

PART 7 – INTERNAL REVIEW

7.1 How does the process of Internal Review operate?

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

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

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

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

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

Council must notify the applicant of the outcome of the review within **14 days** of its determination. A copy of the final review should also be provided to the Privacy Commissioner where it departs from the draft review. Council will provide written notice as to the review rights of the applicant if the internal review is not completed within 60 days from lodgement.

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

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

7.2 What happens after an Internal Review?

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

NCAT can be contacted as follows:

Website: http://www.ncat.nsw.gov.au/
Phone: 1300 006 228
Visit: Level 10 John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

PART 8 – OTHER RELEVANT MATTERS

8.1 Contracts with consultants and other private contractors

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

8.2 Confidentiality

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

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

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

8.3 Misuse of personal or health information

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

8.4 Regular review of the collection, storage and use of personal or health information

The information practices relating to the collection, storage and use of personal or health information is reviewed from time to time. Any new program initiatives will be incorporated into the review process with a view to ascertaining whether or not those programs comply with the PPIPA.

8.5 Regular review of Privacy Management Plan

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

8.6 Alternative complaints process

Should any person wish to have an issue resolved informally, the matter can be considered in accordance with Council's Complaints Handling policy. This policy is available from Council's website. A copy of all of Council's policies, including the complaint handling policy can be accessed on Council's website by clicking here should you require further information or clarification.

8.7 Memorandum of Understandings or Referral Arrangements

As of the date of this plan's endorsement, Council does not have any Memorandums of Understandings or referral arrangements with other agencies.

8.8 Offences

Part 8 of the PIPPA and HRIPA details offences for certain conduct. A table detailing the relevant penalties and associated provision has been provided below:

Offence	Maximum Penalty	Legislative Provision
It is a criminal offence for a public sector official to corruptly disclose and use personal or health information	• Fine of up to 100 penalty units ($11,000), or • Imprisonment for two years, or both	• s 62 of PPIPA • s 68 of HRIPA
It is a criminal offence for a person to offer to supply personal or health information that has been disclosed unlawfully	• Fine of up to 100 penalty units ($11,000), or • Imprisonment for two years, or both	• s63 of PPIPA • s69 of HRIPA
It is a criminal offence for a person – by threat, intimidation or misrepresentation – to persuade or attempt to persuade an individual: • to refrain from making or pursuing a request to access health information, a complaint to the Privacy Commissioner or the NSW Civil and Administrative Tribunal, or an application for an internal review; or • to withdraw such a request, complaint or application.	• Fine of up to 100 penalty units ($11,000)	• s 70(1) of HRIPA
A person must not – by threat, intimidation or misrepresentation – require another person to give consent under HRIPA, or require a person to do, without consent, an act for which consent is required.	• Fine of up to 100 penalty units ($11,000)	• s 70(2) of HRIPA
It is a criminal offence for a person to: • wilfully obstruct, hinder or resist the Privacy • Commissioner or a member of the staff of the Privacy Commissioner • refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner, or • wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of	• Fine of up to 10 penalty units ($1,100)	• s 68(1) of PPIPA

the staff of the Privacy Commissioner • in the exercise of their functions under PPIPA or any other Act		

In addition to the above, under section 308H of the Crimes Act 1900, it is an offence to access or modify restricted data held in a computer where authorisation has not been provided. The maximum penalty for this offence being 2 years.

8.9 Accessibility

The Privacy Management Plan is available on Council's website, available for inspection at Council's Administration Building or upon request, can be mailed out to a nominated postal address.

8.10 Further information

A complaint can be made directly to the Privacy Commissioner through its website or in writing forwarded to the following contact:

The Information Commissioner
By email – ipcinfo@nsw.gov.au
In writing – GPO BOX 7100
SYDNEY NSW 2000
Or by phone – 1800 472 679

For assistance in understanding the processes under the PPIPA and HRIPA, please contact:

1) Privacy Contact Officer
Port Stephens Council
PO Box 42 (116 Adelaide Street)
RAYMOND TERRACE NSW 2324
Phone: (02) 4988 0255
Facsimile: (02) 4988 0130
Email: council@portstephens.nsw.gov.au
Internet: www.portstephens.nsw.gov.au

2) Information and Privacy Commission
Level 11
1 Castlereagh Street
SYDNEY NSW 2000

Phone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Internet: www.ipc.nsw.gov.au

PART 9 – 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 (1) ..... (1) insert full name

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

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

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

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

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

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

.....

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

.....

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

.....
Signature of Applicant

Declared at: .....

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

in the presence of

.....
Name of Justice of the Peace/Solicitor
Who certifies that:
1. *I saw the face of the declarant/deponent OR
   *I did not see the face of the declarant/deponent because he/she was wearing a face covering, but I am satisfied that he/she had a special justification for not removing it, and
2. *I have known the person for at least 12 months OR
   *I confirmed the person's identity with .....

[describe identification document relied on]

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

Appendix 2: Privacy Disclaimer template

YOUR PRIVACY

Port Stephens Council is committed to protecting your privacy. We take reasonable steps to comply with relevant legislation and Council policy.
Purpose: *a statement about why you are collecting the information*.
Intended recipients: *who will be using the information.*
Supply: *legally required OR voluntary.*
Consequence of Non Provision: *what happens if the information is not provided.*
Storage and security: This document will be placed on the relevant file and/or saved in Council's records management system in accordance with Council policy and relevant legislation.
Access: Please contact Council on (02) 4988 0255 to enquire how you can access information.

CONTROLLED DOCUMENT INFORMATION:

This is a controlled document. Hardcopies of this document may not be the latest version. Before using this document, check it is the latest version; refer to Council's website www.portstephens.nsw.gov.au			
RM8 container No	A2004-0135	**EDRMS record No**	
Audience	Public, Council employees, elected Council, volunteers and contractors		
Process owner	Governance Section Manager		
Author	Governance Section Manager		
Review timeframe	Three years	**Next review date**	1 September 2026
Adoption date	June 2000		

VERSION HISTORY:

Version	Date	Author	Details	Minute No.
1.0	June 2000	Legal Officer	Adoption of Privacy Management Plan	
2.0	28 February 2006	Governance Coordinator	Reviewed Privacy Management Plan	432
3.0	10 March 2015	Governance Manager	Reviewed Privacy Management Plan to updated Model Plan from Office of Local Government	050

Version	Date	Author	Details	Minute No.
4.0	28 March 2017	Governance Manager	1. A full compliance review of Plan including the Information & Privacy Commission checklist 2. Remove appendices 2 to 6. 3. Insert new appendix 2 with a privacy disclaimer which replaces those listed in item 2 above. 4. Update appendix 1 with the privacy disclaimer. 5. Reformat public registers into a table for ease of reading page 8 & 9. 6. Delete section 2.5 purpose of public register – now includes within the table listed in item 5 above. 7. Reformatted Privacy Code of Practice in Local Government and Council policy section in Part 3, into a table for ease of reading, from page 13 on. 8. Reformatted Council policy section in Part 3, into a table for ease of reading, from page 38 on. 9. Updated contact details on page 56.	069

Version	Date	Author	Details	Minute No.
5.0	25 August 2020	Governance Section Manager	1. A full compliance review of Plan including the Information & Privacy Commission checklist 2. Section 7.6 updated contact information and the privacy disclosure statement 3. Added 'Section' to reflect amended position title in version control 4. Part 3.6 added 20 working and removed reference to 28 days. 5. Section 3:10 external and related bodies added 'Council employees' 6. Section 5.3 included 'Information and Privacy Commission' and removed 'Office of the Privacy Commission' 7. In part 2 added 'Code of practice' and added hyperlinks to website in the legislative table	164

Version	Date	Author	Details	Minute No.
			8. In Part 3, removed reference to Coastal Protection Act and updated to Coastal Management Act 2016 9. In Part 3, updated Director General's position title to Deputy Secretary of Local Government, Planning and Policy 10. In part 3.2 and 3.3 updated Land Title's Office to Land Registry Services 11. In part 3.11 added 'utility provider' to agency types.	

6.0		Governance Section Manager	Updated numbering, hyperlinks and formatting 1. Added part 6 'Data Breaches' to reflect amendments to PPIPA Act. 2. 6.7 – Added link to Data Breach Policy 3. HPP 5 and IPP 5 – Update of Management Directive titles. Added how the management directive ensures compliance with IPP5. 4. HPP 10 – Added how this can be seen within Council. 5. HPP 13 – Added examples of when a person may elect to remain anonymous and how this request can be made to Council. 6. IPP 9 – Added "This however does not detract from the obligation on Council to take such steps as are reasonable to ensure that any personal information being used is accurate before using it."	

			7. Added part 8.7 ‘Memorandum of Understandings or Referral Arrangements’ to outline any arrangements Council has with other bodies. 8. Added part 8.8 ‘Offences’ to outline the offences under the PPIPA Act 9. Added part 8.9 ‘Accessibility’ to detail how and where this plan can be accessed.	

PORT STEPHENS
COUNCIL

Privacy Management Plan

council@portstephens.nsw.gov.au | 02 4988 0255
PORTSTEPHENS.NSW.GOV.AU