MID-WESTERN REGIONAL COUNCIL

Privacy Management Plan

April 2010

Produced in accordance with section 33(2) of the NSW Privacy and Personal Information Protection Act 1998 and incorporating information related to the NSW Health Records and Information Privacy Act 2002.

Contents

PART 1 INTRODUCTION

This plan outlines how Mid-Western Regional Council handles personal information in accordance with the *Privacy and Personal Information Protection Act* 1989 NSW (PPIP Act) and the *Health Records and Information Privacy Act* 2002 NSW (HRIP Act).

The plan details how the Council deals with the personal information and health information it collects to ensure that it complies with both the PPIP Act and the HRIP Act. In the plan, a reference to 'information' is a reference to both health information and personal information, unless otherwise stated.

This plan is produced in accordance with s 33 of the PPIP Act, it also incorporates the HRIP Act and deals with 4 key issues:

1. The policies and practices that Council has in place to ensure compliance with the PPIP Act and, in particular, the 12 Information Protection Principles.

2. How Council handles public registers.

3. The rights and procedure for internal review.

4. How these policies and practices are circulated throughout Council.

Who does this plan apply to?

Council's privacy management plan applies to:

- Councillors
- Council employees
- Consultants and contractors of Council
- Council owned businesses
- Council committees

What is personal information?

Personal information is defined in s 4 of the PPIP Act as:

'Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.'

This definition includes not only documents held in paper records but also electronic files, video recordings, photographs and genetic characteristics such as fingerprints.

What is not personal information?

Section 4 of the PPIP Act also contains a number of exceptions to the definition of personal information. For example under s 4(3)(b) personal information does not include – *'information about an individual that is contained in a publicly available publication.'*

Examples of such publications include:

- Advertisements that contain personal information in local, city or national newspapers
- Unrestricted personal information on the Internet.
- Books or magazines that are printed and distributed to the public
- Council business papers that are made publicly available.
- Personal information that may form part of a public display which is on view to the general public.

Once personal information is in such publications it is no longer covered by the PPIP Act.

Other exceptions to the definition of personal information include:

- Information about an individual who has been dead for more than 30 years.
- Information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Health Information

Health information is a specific type of personal information that is information, or an opinion, about the physical or mental health or a disability of an individual. It is recognised that collection, access to, use and disclosure of health information are sensitive matters for most individuals and therefore health information must be managed as securely as possible. At the same time there is a public interest in managing appropriate health services for individuals, training health service workers and in conducting health research. Consequently there is a need to be able to share or use health information in a way that protects the individual's rights to privacy. A separate Act (HRIP) was passed to enable both protection for individuals and appropriate use of health information.

Examples of the types of health information held by Council.

Records about staff:

- Sick Leave applications (with or without medical certificates)
- Worker's compensation records
- Rehabilitation Records

Records about residents:

- Childcare records (including immunisation and medical histories)

Information released under other legislation

Council is also required to make certain information publicly available under other legislation. The *Government Information (Public Access) Act 2009* (GIPA Act) sets out a number of documents that Council must make available to the public as "open access information" as defined in s18 and schedule 1 of schedule 5 of the GIPA Act. These include annual reports, management plans and development applications.

Information that is held by Council that is not defined as open access information may be released under the GIPA Act by Council subject to application. More information on accessing information under this Act can be found in Council's Access to Information policy. This is available on council's website.

If there are inconsistencies between the PPIP Act and other legislation such as the GIPA Act, the requirements of these other Acts generally prevail over the PPIP Act.

What types of personal information are held by Council?

Council holds personal information about Councillors, ratepayers, customers, residents and employees.

Councillors:

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

Customers, ratepayers and residents:

- name and home addresses of individuals
- property ownership details and information about concessions
- personal information relating to the processing of development applications
- bank account details
- information about families of children at child care centres.

Employees:

- information obtained during recruitment
- leave and payroll data
- personal contact information
- performance management plans
- disciplinary matters
- pecuniary interest returns
- wage and salary entitlements.

Privacy Contact Officer

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

- receive advice and updated information from Privacy NSW about the implementation of the Privacy and Personal Information Protection Act 1998 and the Health Records Information Protection Act 2002

- act as a first point of contact with Privacy NSW for all matters related to privacy and personal information

- act as a focal point within their organisation for all matters related to privacy and personal information

- act as a first point of contact for members of the public for all matters related to privacy and personal information.

- disseminating information on privacy issues within the organisation

- co-ordinating the implementation of the privacy legislation in their organisation, including drawing up and reviewing Privacy Management Plans

- providing privacy training for staff about whether information is "personal information" or "health information" as defined in the legislation

- ensuring that all complaints about privacy breaches and internal reviews are dealt with in the proper manner

PART 2 PUBLIC REGISTERS

Council is required to hold and maintain public registers under various legislation and make them available for inspection.

What is a public register?

A public register is defined in s 3 of the PPIP Act as:

'A register of personal information that is required by law to be, or is made, publicly available or open to public inspection.'

What is a non public register?

A non public register is still a register, but it is not a public register for the purposes of the PPIP Act. Such a register may not be publicly available or may not contain personal information. An example of such a register is the Companion Animals Register.

Types of public registers held by Council

Under the LGA Council holds a number of registers including land registers, records of approval, and register of pecuniary interests.

Under the Environmental Planning and Assessment Act Council also holds public registers such as the register of consents and approvals and the record of building certificates.

Disclosure requirements under the PPIP Act

When disclosing personal information contained in public registers, Council will comply with Part 6 of the PPIP Act and the Privacy Code of Practice for Local Government ('the code').

Under s 57(1) of the PPIP Act, personal information must not be disclosed unless Council is satisfied that access is for a purpose related to the purpose for which the register is kept.

As part of this process, Council may ask the person requesting access what they intend to use the information for. This may need to be given in the form of a statutory declaration.

If the purpose stated by the applicant does not match the purpose for which the register is kept, access to the information will not be given.

If the personal information is in a publicly available publication then it will not be covered by the PPIP Act.

Modification under the code

Under the code, Council may allow any person to inspect a publicly available copy of a public register in Council premises – and copy a single entry or a page of the register – without requiring them to provide a reason for accessing the register. In this case Council will not need to determine whether the proposed use is consistent with the purpose for which the register is kept.

Council will not require reasons why someone is inspecting Council's pecuniary interest register or any register on which Council records declarations made by councillors or designated officers under Ch 14 Part 2 Divisions 3 or 4 of the LGA.

Requests for access, copies or sale of the whole or substantial part of a public register held by Council may not fit the purpose for which the register was created. As a result Council may:

- not disclose names and addresses of both current and previous property owners and applicants

- require a statutory declaration from the person requesting the information to satisfy Council that the purpose of use is consistent with the purpose for which the register is kept.

Government Information (Public Access) Act

Section 57 of the PPIP Act prevails over schedule 5 of the GIPA Act if there is any inconsistency. Therefore:

1. If a register is listed in schedule 5 of the GIPA Act, access must not be given except in accordance with s 57(1) of the PPIP Act.

2. If a register is not listed in schedule 5 of the GIPA Act, access must not be given unless:

   (i) it is allowed under s 57(1) of the PPIP Act; and
   (ii) inspection is not contrary to the public interest (s 14 of the GIPA Act).

Suppression

An individual may request that their personal information is removed from, or not placed on, a publicly available register and not disclosed to the public.

Council will do this if it is satisfied that the safety or wellbeing of any person would be affected if the personal information requested to be suppressed were not. However Council will not suppress if we believe that the public interest in maintaining access to the information outweighs any individual interest in suppressing the information.

If information is suppressed, it may be kept on the register for other purposes.

PART 3 PIPP ACT INFORMATION PROTECTION PRINCIPLES

What are the Information Protection Principles?

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

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

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

This section of the plan includes:

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

Information Protection Principle 1 – Section 8 of the PPIP Act: Collection of personal information for lawful purposes

Council will only collect personal information that is reasonably necessary for a lawful purpose as part of its proper functions.

Personal information will not be collected by unlawful means. If private contractors or consultants are engaged by Council and they are involved in collecting personal information, they must agree not to do so by unlawful means.

Council's major functions and obligations are governed by the *Local Government Act* 1993 ('LGA'). Council also has a number of functions under other Acts. These Acts are listed in s 22 of the LGA and include the Companion Animals Act, Library Act and the Swimming Pools Act.

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

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

Information Protection Principle 2 – Section 9 of the PPIP Act: Collection of personal information directly from the individual

When Council collects personal information this will be directly from the individual concerned unless:

- The individual has authorised collection from someone else.
- The information relates to a person who is under 16 years of age and has been provided by a parent or guardian.

Council collects personal information through the various forms that customers complete and lodge with Council. Some examples include:

- Compilation or referral of registers
- customers completing and lodging development application forms
- access to information requests
- companion animal registration
- applications for inspections or certifications.

Unsolicited information

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

Exemptions under the PPIP Act

Council is not required to comply with IPP 2 if:

- The information has been collected in connection with proceedings (whether or not they have actually started) before any court or tribunal [s 23(2)].
- Council is 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 compliance might detrimentally affect or prevent the proper exercise of Council's complaint handling or investigative functions [s 24(4)].
- Council is lawfully authorised or required not to comply with the principle concerned [s 25(a)].
- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].
- Compliance by Council would, in the circumstances, prejudice the interests of the individual to whom the information relates [s 26(1)].

Modification under the code

Council can depart from IPP 2 if indirect collection of personal information is reasonably necessary to confer an award, prize, benefit or similar form of personal recognition to the individual to whom the information relates.

Information Protection Principle 3 – Section 10 of the PPIP Act: Requirements when collecting personal information:

Council will ensure that when collecting personal information directly from individuals they are told that:

- the information is being collected
- the purpose of collecting the information
- who the intended recipients are
- whether supplying the information is voluntary or required by law
- the consequences to the individual if the information is not provided
- their rights to access and correct the information
- the name and address of the agency collecting the information and the agency that will be holding the information.

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

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

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

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

Before Council adopts a new form, a draft will be reviewed by the appropriate officer to ensure it complies with IPP 3 and 4.

In addition to the PPIP Act, Council has adopted an Access to Information policy which provides that the names of people who complain to Council remain confidential. Complainants are made aware that their details will remain confidential and will not be disclosed. All requests for access to information are subject to this policy. A copy of this policy can be obtained from Council's website.

Exemptions under the PPIP Act

Council is not required to comply with IPP 3 if:

- The information concerned is collected for law enforcement purposes [s 23(3)].

- Council is 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 compliance might detrimentally affect or prevent the proper exercise of Council's complaint handling or investigative functions [s 24(4)].

- Council is lawfully authorised or required not to comply with the principle concerned [s 25(a)].

- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].

- Compliance by Council would, in the circumstances, prejudice the interests of the individual to whom the information relates [s 26(1)].

- The individual to whom the information relates has expressly consented to Council not complying with IPP 3 [s 26(2)].

Modification under the code

Council can depart from IPP 3 if indirect collection of personal information is reasonably necessary to confer an award, prize, benefit or similar form of personal recognition to the individual to whom the information relates.

Obligations under other legislation

Council also incurs obligations under other legislation in relation to collecting personal information. For example, the Workplace Surveillance Act 2005 requires Council to notify employees of all surveillance in the workplace which may be carried out by Council.

Information Protection Principle 4 – Section 11 of the PPIP Act: Other requirements relating to collection of personal information:

When Council collects personal information it will take reasonable steps in the circumstances to ensure that:

- the information is relevant to that purpose, is accurate, up-to-date, complete and not excessive

- when collecting the information the personal affairs of the individual are not unreasonably intruded on.

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

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

Information Protection Principle 5 – Section 12 of the PPIP Act: Retention and security of personal information

Council will ensure that:

- information is not kept for longer than is necessary for the purpose for which it may lawfully be used

- information is disposed of securely

- information is protected against loss, unauthorised access, use, modification, disclosure and all other misuse by undertaking reasonable security safeguards

- if it is necessary for Council to give information to a person in connection with the provision of a service to Council, everything reasonable will be done within Council's powers to prevent unauthorised use or disclosure.

To ensure information is held securely:

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

Council also has in place an Acceptable Use of IT Services which sets out the requirements in relation to IT security.

Council's code of conduct (clause 10.8) also sets out the obligations that exist in relation to dealing with personal information. This includes a definition of what personal information is and the relevant legislation and policies that need to be complied with.

Information Protection Principle 6 – Section 13 of the PPIP Act: Information about personal information held by agencies

Council will take reasonable steps to enable individuals to determine whether Council holds personal information relating to them. If Council does hold such information, upon request, Council will advise the individual of:

- the nature of the information
- the purpose for which it is being used
- their entitlement to gain access to the information.

Modification under the GIPA Act

IPP 6 is modified by s 20(5) of the PPIP Act with the importation of the relevant sections of the GIPA Act. The effect of this is that relevant sections of the GIPA Act are treated as being part of the PPIP Act. Therefore when an application is made under IPP 6, Council must consider these sections of the GIPA Act.

When Council receives a request under IPP 6 a search will be undertaken of Council records. The applicant may be asked to describe the dealings they have had with Council to assist the searching process. A response to applications under IPP 6 will ordinarily be made within 20 working days.

Exemptions under the PPIP Act

Council is not required to comply with IPP 6 if:

- Council is lawfully authorised or required not to comply with the principle concerned [s 25(a)].
- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].

Reporting

Several reporting requirements exist under the privacy regimes. These include:

- Section 33 (3) of the PPIP Act requires that the Council's Annual Report include a statement regarding actions taken by the Council to comply with the requirements of the Act. Statistical details must also be given of any reviews (internal and external by the Administrative Decisions Tribunal) conducted by or on behalf of the Council.
- The Council is required to publish a Privacy Management Plan under section 33(1) of the PPIP Act and amend it from time to time. A copy is to be forwarded to the NSW Privacy Commissioner each time it is amended.

Information Protection Principle 7 – Section 14 of the PPIP Act: Access to personal information held by agencies

Council will ensure that individuals are provided access to personal information held by Council within 20 working days. Requests for access should be made in writing and addressed to the General Manager.

If employees of Council seek access to records held about them, such requests need to be directed to the Manager Human Resources.

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

1. An individual's personal information is in documents which also have information about others

2. Access is sought for information about someone else.

Exemptions under the PPIP Act

Council is not required to comply with IPP 7 if:

- Council is lawfully authorised or required not to comply with the principle concerned [25(a)].

- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].

Modification under the GIPA Act

Like IPP 6, IPP 7 is also modified by s 20(5) of the PPIP Act with the importation of the relevant sections of the GIPA Act.

Staff records

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

Information Protection Principle 8 – Section 15 of the PPIP Act: Alteration of personal information:

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

Changes to personal information will require appropriate supporting documentation. The amount of documentation required will depend on how substantive the proposed amendments are. No charges are required in relation to amendments under IPP 8.

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

If Council refuses to make the requested amendments, Council may attach a notation to the information if this is requested by the individual.

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

Modification under the GIPA Act

Like IPP 6 & 7, IPP 8 is also modified by s 20(5) of the PPIP Act with the importation of the relevant sections of the GIPA Act.

The GIPA Act is not affected by the operation of the PPIP Act. Applications to amend records can only be made under the PPIP Act.

Exemptions under the PPIP Act

Council is not required to comply with IPP 7 if:

- Council is lawfully authorised or required not to comply with the principle concerned [s 25(a)].

- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].

Information Protection Principle 9 – Section 16 of the PPIP Act: Agency must check the accuracy of personal information before use:

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

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

Information Protection Principle 10 – Section 17 of the PPIP Act: Limits on use of personal information

Council will not use personal information for a purpose other than that which it was collected for unless:

- the individual has consented to such use
- the other purpose it is being used for is directly related to the purpose for which it was collected
- the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual who the information relates to or another person.

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

Exemptions under the PPIP Act

Council is not required to comply with IPP 10 if:

- Use for another purpose is reasonably necessary for law enforcement purposes or for the protection of the public revenue [s 23(4)].
- Use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in order to enable Council to exercise its complaint handling functions and compliance might detrimentally affect or prevent the proper exercise of Council's complaint handling or investigative functions [s 24(2)].
- Council is lawfully authorised or required not to comply with the principle concerned [s 25(a)].
- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].
- Disclosure is by a public sector agency 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 by a public sector agency 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 [s 28(3)].

Modification under the code

Council can depart from IPP 10 if:

- 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.
- The personal information is to be used to confer an award, prize, benefit or similar form of personal recognition on a particular person.

Information Protection Principle 11 – Section 18 of the PPIP Act: Limits on disclosure of personal information

Council will not disclose information to a person or body (other than the individual to whom the information relates) unless:

- The disclosure is directly related to the purpose for which the information was collected.

- Council has no reason to believe that the individual would object to disclosure.

- The individual concerned is reasonably likely to be aware, or has been made aware in accordance with IPP 3 (section 10) that this kind of information is usually disclosed to that other person or body.

- Council believes on reasonable grounds that disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual who the information relates to or another person.

If Council does disclose personal information in accordance with IPP 11 to a person or public sector agency they must not use or disclose the information for a purpose other than that which it was given to them for.

Exemptions under the PPIP Act

Council is not required to comply with IPP 11 if:

- the disclosure of the information concerned:

  - is made in connection with proceedings for an offence or for law enforcement purposes (including the exercising of functions under or in connection with the *Confiscation of Proceeds of Crime Act 1989* or the *Criminal Assets Recovery Act 1990*), or

  - 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

  - is authorised or required by subpoena or by search warrant or other statutory instrument, or

  - is reasonably necessary:
    for the protection of the public revenue, or
    in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed [s 23(5).

- Council is investigating a complaint that could be referred or made to, or has been referred from or made by, an investigative agency, and if such use is necessary in order to enable Council to exercise its complaint handling or investigative functions [s 24(4)].

- Council is lawfully authorised or required not to comply with the principle concerned [s 25(a)].

- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].

- If the individual to whom the information relates has expressly consented to Council not complying with IPP 11 [s 26(2)].

Modification under the code

Council can depart from IPP 11 in the following 3 circumstances:

1. Council may disclose personal information to public sector agencies or public utilities if:

   (i) the agency has approached Council in writing
   (ii) Council is satisfied that the information is to be used by the agency for its proper and lawful functions
   (iii) Council is satisfied that the personal information is reasonably necessary for the exercise of that agency's functions.

2. The personal information collected about an individual is to be disclosed for the purpose of giving that person an award, prize, benefit or similar form of personal recognition.

3. If 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 exemption does not allow Council to give an opinion about that person's suitability for a particular position with any potential employer. However this does not apply where Council is satisfied that the person has provided their consent for Council to provide a reference.

Effect of other legislation

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

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

Subpoenas and similar court orders for documents

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

All subpoenas and similar court orders are to be directed to the Council's Manager Governance. Individual departments or officers must not accept or deal with subpoenas or

other orders except as directed by the General Manager.

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

Requests from police and law enforcement agencies

Members of staff receiving requests for personal information from law enforcement agencies must direct those requests to the Manager Governance as the Council's Privacy Contact Officer. The decision regarding disclosure of personal information will be made by the Council's Privacy Contact Officer. This procedure does not apply in cases where there is an imminent threat to life or safety, however even then reasonable attempts should be made to discuss the matter with the Privacy Contact Officer.

Tax file numbers

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

Information Protection Principle 12 – Section 19 of the PPIP Act: Special restrictions on disclosure of personal information

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

Council will not disclose personal information to any person or body in a Commonwealth agency or jurisdiction outside NSW unless:

- a relevant privacy law is in force in that jurisdiction and applies to the personal information concerned or applies to the Commonwealth agency

- the disclosure is permitted under a privacy code of practice.

Modification under the code

If Council is asked for information 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 exemption does not allow Council to give an opinion as to that person's suitability for a particular position with any potential employer. However this does not apply if Council is satisfied that the person has provided their consent for Council to provide a reference.

Exemptions under the PPIP Act

Council is not required to comply with IPP 12 if:

- The disclosure of the information is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed [s 23(7)].

- Council is lawfully authorised or required not to comply with the principle concerned [s 25(a)].

- Non compliance is otherwise permitted under an Act or any other law [s 25(b)].

- If the individual to whom the information relates has expressly consented to Council not complying with IPP 12 [s 26(2)].

PART 4 HRIP ACT INFORMATION PROTECTION PRINCIPLES

In 2002, most reference to 'health information' was taken out of the PPIPA and separate legislation, 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
- 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. Council will often hold health information by reason of its role in elder care, child care and various types of community health support services. It is therefore very important that Council is familiar with the 15 Health Protection Principles ("HPP") set down in Schedule 1 to the HRIPA. Each of these HPPs are considered below.

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

Health Privacy Principle 1

Purposes of collection of health information

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

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

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

Health Privacy Principle 2

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

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

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

Health Privacy Principle 3

Collection to be from the individual concerned

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.
(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

Health Privacy Principle 4

Individual to be made aware of certain matters

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

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

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

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

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

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

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

prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

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

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

(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a 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).

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.

(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).

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

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

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

Health Privacy Principle 8

Amendment of health information

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

(a) is accurate, and

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

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

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

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

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

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

Health Privacy Principle 9

Accuracy

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

Council Policy

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

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

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

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

Health Privacy Principle 10

Limits on use of health information

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

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

(b) 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,

(c) 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) 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) 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) 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

(g) 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) 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 health registration Act, 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) 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) 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) the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

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

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

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

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

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

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

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

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

Council policy

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

Health Privacy Principle 11

Limits on disclosure of health information

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

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

(b) 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

(c) 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) 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) 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) 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) 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) 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) 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 health registration Act, 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) 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) 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) the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

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

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

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

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

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

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

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

Council Policy

Council will only disclose health information under the following circumstances:

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

Health Privacy Principle 12

Identifiers

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

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

(a) the individual has consented to the adoption of the same identifier, or
(b) the use or disclosure of the identifier is required or authorised by or under law.

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

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)-(k) or 11 (1) (c)-(l), or
(b) the individual has consented to the use or disclosure, or
(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

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

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

Council Policy

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

Health Privacy Principle 13

Anonymity

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

Council Policy

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

Health Privacy Principle 14

Transborder data flows and data flow to Commonwealth agencies.

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

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or
(b) the individual consents to the transfer, or
(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or
(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or
(e) all of the following apply:

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

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

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

(g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or
(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

Council Policy

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

Health Privacy Principle 15

Linkage of health records

(1) An organisation must not:

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

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

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

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

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

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

(3) In this clause:

"health record" means an ongoing record of health care for an individual.

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

Council Policy

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

PART 5 RELEVANT POLICIES

There are various policies and protocols that affect the handling of personal information by Mid-Western Regional Council:

Access to Information Policy

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

Acceptable Use of IT Services Policy

Outlines responsibilities when using computers for email and internet.

Records Management Policy

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

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

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

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

- staff are not to maintain individual or separate files or unauthorised record keeping systems;

- no records are to be disposed of unless authorised by the Records Section and are covered by a disposal schedule authorised by State Records; or under relevant legislation as directed in part 3 of the Act; or through 'normal administrative practice' as defined in the Act. This applies to electronic records as well as 'hardcopy' records. Records disposal is addressed in more detail later;

- only authorised staff may create new files or modify or close existing files or record file movements on the authorised organisational records system;

- the location of every record should be accurate and up to date at all times. Staff are responsible for recording location changes when passing a file to another staff member, by notifying the responsible records person;

- no file should be removed from the records administration area without informing a records staff member so that records can be updated;

- staff should minimise the number of files kept on desks/in workstations and the length of time they are kept;

- files should not leave the premises, apart from exceptional circumstances and then only if authorised by a senior manager. If possible, a photocopy of relevant documents should be taken to meetings offsite. The records administration area should be informed when files are removed from the premises; and

- records including electronic files, email or other computer based information must not be removed from the network without the appropriate authorisation form being completed and approved.

PART 6 INTERNAL REVIEW

Requesting an internal review

If a person is aggrieved by Council's conduct they are entitled to an internal review under s 53 of the PPIP Act.

Under s 52 of the PPIP Act a review can only be undertaken where it is alleged that Council has:

- contravened any of the IPPs
- contravened the code of practice which applies to Council
- disclosed personal information contained in a public register.

Applications for review can only be made within 6 months of the complainant being first aware of the conduct. Council may accept a complaint after this time, however, is not required to. Applications need to be in writing and addressed to the Privacy Contact Officer. A privacy complaint internal review application form can be obtained from Privacy NSW website.

The internal review process

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

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

• the applicant;
• the Privacy Commissioner.

There is a checklist which provides a model of the internal review process available at the website of NSW Privacy at
http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_publications

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

1. Send the complainant an acknowledgment letter setting out who the officer undertaking the review is, the date for completion, and any other relevant information relating to the review.

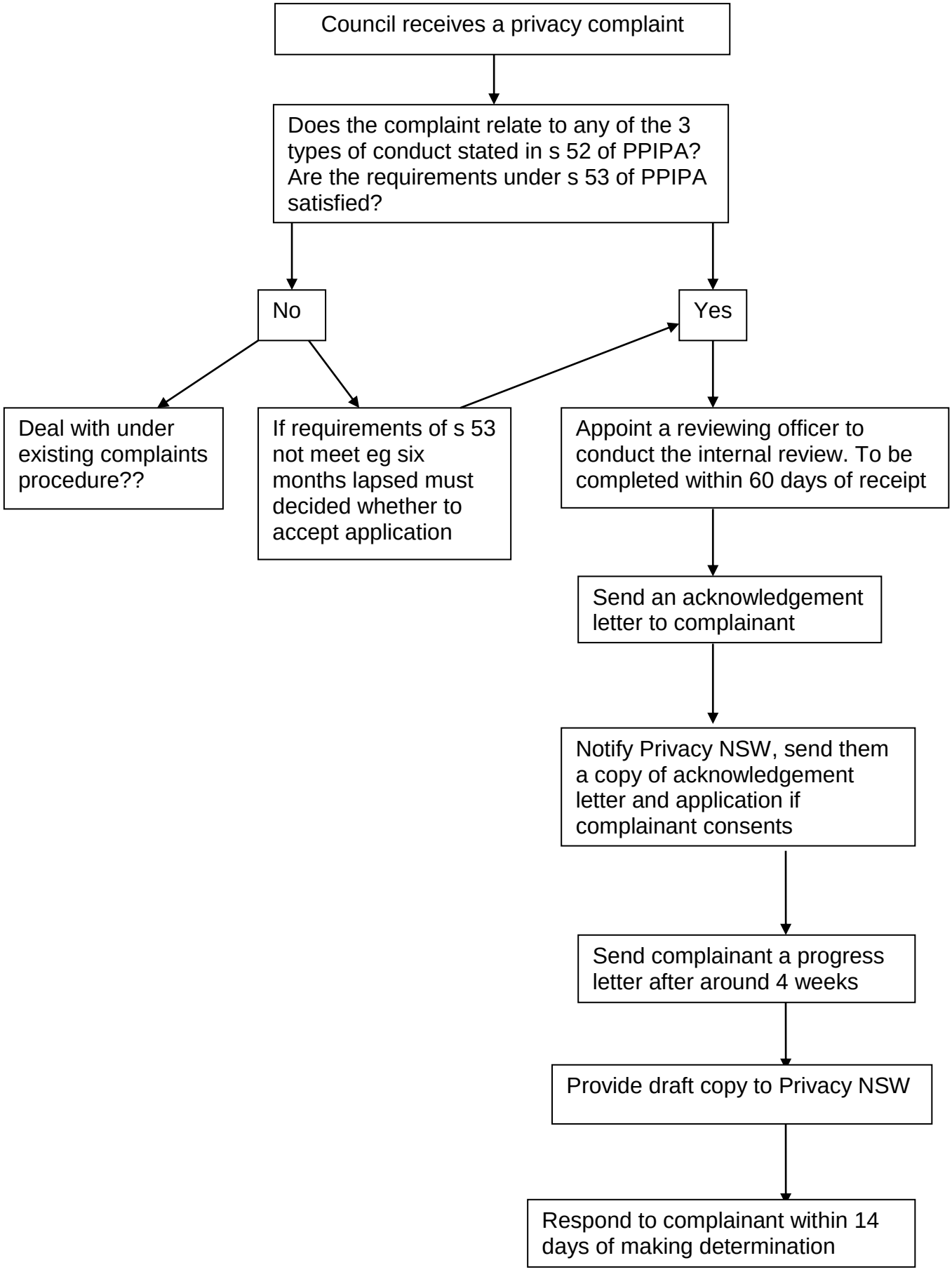
2. Notify Privacy NSW of the complaint and if the complainant consents, send them a copy of the application. A copy of the acknowledgment letter will also be provided to them. In addition, the NSW Privacy Commissioner is entitled to make submissions to Council in relation to the application.

3. Send the complainant a progress letter approximately four weeks after the acknowledgment letter. This letter will contain details of how the review is progressing, when it will be completed, and a reminder of the rights of review to the Tribunal if the review is not completed within the 60 day timeframe.

4. Provide a draft copy of the preliminary determination to Privacy NSW for their comment and response before sending the determination to the complainant.

5. A summary of the findings of the review must be provided to the Privacy Commissioner within 14 days of its completion

Privacy internal review process



Conduct following an internal review

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

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

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

Options after an internal review

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

PART 7 TRAINING AND EDUCATION

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

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

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

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

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

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