

# Parliamentary Counsel's Office Privacy Management Plan

## Introduction

The *Privacy and Personal Information Protection Act 1998* (the PPIP Act) requires a public sector agency to prepare and implement a privacy management plan. Such a plan is a written statement by the agency of how it plans to comply with the requirements of the Act. This document is the privacy management plan for the Parliamentary Counsel's Office.

The PPIP Act provides that personal information held by a public sector agency is protected by a number of information protection principles set out in Part 2 of the Act. Those principles relate to the collection, storage, use and disclosure of personal information.

In addition, the *Health Records and Information Privacy Act 2002* (the HRIP Act) applies a number of health privacy principles specifically to the collection, storage, accuracy, use and disclosure of health information. Information covered by the HRIP Act is dealt with on page 5 of this Plan.

## Definition of “personal information”

The PPIP Act defines personal information to mean information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Accordingly, a person does not have to be clearly identified by the information. It is enough if a person's identity can reasonably be ascertained from the information.

The PPIP Act also provides that the definition of personal information does **not** include certain information, such as information about an individual:

- contained in a publicly available publication (for example a newspaper or Hansard), or
- contained in, or collected in the course of investigating, a protected disclosure made by a whistleblower under the *Protected Disclosures Act 1994*, or
- arising out of a Royal Commission or Special Commission of Inquiry, or
- arising out of a complaint made under Part 8A of the *Police Act 1990*, or
- contained in a Cabinet document or Executive Council document, as those documents are defined as exempt documents by the *Freedom of Information Act 1989*, or
- concerning an individual's suitability for appointment or employment as a public sector official.

## Information protection principles

The PPIP Act provides that all public sector agencies are to comply with the information protection principles contained in Part 2 of that Act. The **information protection principles** set out in sections 8 to 11 of the PPIP Act relate to the **collection** of personal information by a public sector agency. Those principles generally provide that:

- personal information may only be collected for a lawful purpose and may only be collected directly from the individual or their parent or guardian, and
- the individual concerned is to be made aware of certain things such as the purpose of collection and intended recipients of the personal information, and
- the personal information collected must be relevant for the purpose for which it is collected, must not be excessive and must be accurate, up-to-date and complete.

It should be noted that section 4 (5) of the PPIP Act provides that, for the purposes of the Act, personal information is not **collected** by a public sector agency if the receipt of the information by the agency is unsolicited.

In order to determine the types of personal information that are collected by the Parliamentary Counsel's Office (PCO), it is necessary to look at its functions. As a separate office within the Department of Premier and Cabinet, the PCO is a central agency that has the primary role of providing a legislative drafting and publishing service to Government. The PCO's services are explained in the relevant chapter of the Department of Premier and Cabinet's Annual Report and an extract from this document is available from PCO's Internet site ([www.pco.nsw.gov.au](http://www.pco.nsw.gov.au)).

The PCO does not collect personal information from members of the public as any part of its operations and, apart from responding to inquiry calls about the status of legislation, has virtually no direct contact or correspondence with the public.

However, although the PCO does not collect personal information within the meaning of the Act, all officers are to comply as far as possible with the above principles, as modified by the code of practice dealing with inter-agency transfers of personal information (see below).

The PCO receives some personal information via email through the NSW Legislation Website, which is maintained by the PCO. This consists of e-mail addresses and contact details for individuals making enquiries about the status of legislation or subscribing to the weekly notification of legislative activity service that the PCO provides via email. The PCO's Internet site includes a message to the following effect:

“The NSW Parliamentary Counsel's Office respects your privacy. Any personal information provided to this Office will be handled in accordance with the *Privacy and Personal Information Protection Act 1998*.”

Apart from the list server used to email subscribers copies of the weekly notification of legislative activity, there is no other systematic collection of personal information via email.

The **information protection principle** set out in section 12 of the PPIP Act relates to the retention and security of personal information. The principle requires that:

- the information is kept for no longer than necessary for the purposes for which it may lawfully be used, and
- the information is disposed of securely, and
- security safeguards are in place to protect against loss, unauthorised access, use, modification, disclosure and all other misuses, and
- if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, the agency has done everything reasonably in its power to prevent unauthorised use or disclosure of the information.

This principle does not amount to an authorisation to destroy or dispose of records once they are no longer useful. Agencies still have to comply with the provisions of the *State Records Act 1998*, which covers the disposal of State records.

It should be noted that a range of corporate services is provided to the PCO by ServiceFirst of the Department of Commerce. These services include personnel services and records management services. Accordingly, the Department of Commerce will be required to prepare

a privacy management plan setting out how the Department, including ServiceFirst, plans to comply with the requirements of the Act. ServiceFirst will be required to comply with that privacy management plan when providing personnel and records management services to the PCO.

As well as ServiceFirst complying with this principle in the course of undertaking records management on behalf of the PCO, all officers should be aware that where personal information is retained by the PCO:

- it should be kept secure on the appropriate file, and
- officers should take appropriate action to ensure that there is no unauthorised access to the personal information, and that it is not lost, modified, wrongly disclosed or otherwise misused, and
- files should be disposed of by ServiceFirst in accordance with the provisions of the *State Records Act 1998* and the privacy management plan governing ServiceFirst prepared by the Department of Commerce, and
- if personal information is given to a person in connection with the provision of a service to the PCO, the responsible PCO officer is to take all necessary action to ensure that the information is not to be used or disclosed for any other purpose. Any contract should contain a provision preventing the contractor using the personal information for any other purpose and requiring the return of all personal information once the service is completed.

In relation to the security and appropriate use of any personal information held by the PCO, all officers should refer to the provisions of the PCO's Code of Conduct.

The **information protection principles** set out in sections 13, 14 and 15 of the PPIP Act generally provide that agencies are required to:

- take steps to enable any person to **ascertain** whether the agency holds personal information relating to the person and, if so, the nature of the information, the main purposes for which it is used and the person's entitlement to gain access to the information, and
- provide **access** to the personal information, at the request of the person to whom the information relates, to that person, and
- make appropriate **amendments** to ensure that the personal information is accurate, relevant, up-to-date, complete and not misleading, and
- if not prepared to make such amendments, then at the request of the individual concerned, **attach** to the personal information any statement provided by that individual of the amendment sought.

These principles are designed to alert people to the fact that an agency may hold information, allow them a right of access to their personal information as well as a right to amend or attach a statement if they believe the personal information to be incorrect.

Any person may apply to the PCO to ascertain whether it holds personal information relating to that individual. Applications for access should be made in writing and directed to:

The Privacy Contact Officer  
Parliamentary Counsel's Office  
Level 23 AMP Centre  
50 Bridge Street  
Sydney NSW 2000

The Privacy Contact Officer will be responsible for liaising with the person seeking access to personal information and taking appropriate steps to comply with the information protection principles set out in sections 13, 14 and 15 of the PPIP Act.

It should be noted that the PPIP Act provides that the provisions of the *Freedom of Information Act 1989* imposing limitations on the disclosure of documents apply in relation to applications for access to personal information under the PPIP Act.

Accordingly, the FOI exemptions will need to be considered when deciding whether to provide access to personal information in accordance with sections 13, 14 and 15 of the PPIP Act. The FOI contact officer should be consulted in relation to the applicability of such exemptions. Any decision regarding the provision of access to personal information, or the making of amendments to such information, will be made by the Parliamentary Counsel or Deputy Parliamentary Counsel.

The **information protection principle** set out in section 16 of the PPIP Act provides that a public sector agency that holds personal information must not **use** the information without taking reasonable steps 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.

It is a matter for officers to determine what is a reasonable and appropriate level of checking based on their knowledge of the information and the procedures used to collect the information. Each officer within the PCO is, in the course of carrying out his or her functions, to take responsibility for considering the purpose for which any personal information is to be used and then ensure that for that purpose it is relevant, accurate, up-to-date, complete and not misleading.

The **information protection principles** set out in sections 17, 18 and 19 of the PPIP Act deal with the **limits on the use and disclosure** of personal information collected or held by public sector agencies. "Use" refers to the treatment and handling of personal information within the agency, and "disclosure" relates to making personal information available to persons, bodies or other agencies.

It should be noted that section 28 (3) (a) of the PPIP Act provides that nothing in section 17, 18 or 19 prevents or restricts the disclosure of information by a public sector agency to another agency administered by the same Minister. Accordingly, the Act does not prevent the exchange of personal information between PCO and the other parts of the Department of Premier and Cabinet (such as General Counsel) as well as other agencies administered by the Premier. Section 28 (3) (b) of the PPIP Act provides that nothing in section 17, 18 or 19 prevents a public sector agency disclosing personal information to an agency administered by the Premier for the purpose of informing the Premier about any matter. Accordingly, sections 17, 18 and 19 do not prevent other public sector agencies from disclosing personal information to the PCO for the purpose of informing the Premier about any matter.

In the event that the PCO discloses personal information to other public sector agencies in the course of carrying out its functions, the practice is addressed in the code of practice dealing with inter-agency transfers made by the Attorney General (see below).

It should be noted that the PPIP Act also provides that a public sector agency is not required to comply with the information protection principles (excluding section 11 relating to collection of personal information, and section 12 relating to retention and security of personal information) if non-compliance is permitted under another Act. An example of another Act permitting such non-compliance would be the *Victims Rights Act 1996*, which provides that a victim of crime is entitled to certain information including personal information regarding the accused. Accordingly, officers need to consider, when carrying out their functions, whether the provisions of another Act may permit non-compliance with any of the information protection principles.

## **Privacy codes of practice**

The PPIP Act provides that an agency may make a privacy code of practice in order to modify the agency's obligations under the information protection principles. It is not anticipated that the PCO will prepare a privacy code of practice. However, the Attorney General has made a privacy code of practice dealing with inter-agency transfers of personal information. The code applies to the PCO and should be read in conjunction with this privacy management plan. A copy of the code is attached.

## **Public registers**

Part 6 of the PPIP Act provides that a public sector agency that keeps a public register must not disclose personal information kept in the register except for the purposes for which the register is kept or for the purposes of the Act under which the register is kept. The PPIP Act defines a public register to be any register of personal information that is required by law to be, or is made, publicly available or open to public inspection. As the PCO does not keep any public registers within the meaning of the Act, Part 6 of the Act does not apply to the PCO.

## **Health Records and Information Privacy Act 2002**

The HRIP Act applies to all private and public sector organisations and specifically covers health information. "Health information" is defined in section 6 of that Act and includes personal information that is information or an opinion about the physical or mental health or a disability of an individual.

Information handled by the PCO as part of its core business is generally outside of this definition and is therefore not covered by the HRIP Act. However, a range of human resources and management information may be covered by this definition, including:

- medical certificates and other information submitted in support of sick leave applications,
- records relating to workers compensation claims,
- records of other workplace incidents requiring first aid,
- medical or disability information supplied by applicants during the staff recruitment process,
- health information provided by employees to supervisors, grievance officers or the Parliamentary Counsel during performance management or grievance discussions,
- personnel records relating to use of sick leave forming part of the Workforce Profile collection.

The HRIP Act provides that such information is to be handled in accordance with the 15 health privacy principles set out in Schedule 1 of that Act and any relevant health privacy codes of practice. Those principles are similar to those under the PPIP Act and are summarised as follows:

### Collection

- 1 **Lawful:** collection must be for a lawful purpose and only if it is directly related to the organisation's activities and is necessary for that purpose.
- 2 **Relevant:** health information must be relevant, not excessive, accurate, up-to-date and complete.
- 3 **Direct:** health information must only be collected directly from the person concerned unless it is unreasonable or impracticable to do so.
- 4 **Open:** explain why you are collecting health information, what you will do with it and who else might see it.

### Storage

- 5 **Secure:** health information must not be kept for any longer than necessary, must be disposed of appropriately and must be kept securely.

### Access & Accuracy

- 6 **Transparency:** explain to the person what health information about them is being stored, why it is being used and any rights they have to access it.
- 7 **Accessible:** allow people to access health information without excessive delay or expense.
- 8 **Correct:** allow people to correct, delete or add to their health information where necessary.
- 9 **Accurate:** ensure that the health information is relevant, accurate, up-to-date, complete and not misleading before using it.

### Use

- 10 **Limited:** only use health information for the purpose for which it was collected, or a directly related purpose that the person would expect.

### Disclosure

- 11 **Limited:** only disclose health information for the purpose for which it was collected, or a directly related purpose that the person would expect.

### Identifiers and Anonymity

- 12 **Not identified:** only identify people by using unique identifiers if reasonably necessary to carry out your functions efficiently.
- 13 **Anonymous:** give people the option of receiving services from you anonymously, where this is lawful and practicable.

### Transferrals and Linkages

- 14 **Controlled:** the transfer of health information to a jurisdiction outside NSW and to Commonwealth agencies must be controlled in accordance with this principle.
- 15 **Authorised:** people must expressly consent to participate in any system that links health records across more than one organisation.

The PCO's procedures for the collection, storage, use, disclosure and destruction of health information comply with the above health privacy principles. The PCO will regularly review those procedures to ensure compliance is maintained.

## **Distribution and communication of plan**

A copy of this privacy management plan will be made available to each person within the PCO. The plan will also be available electronically on the PCO's Internet and Intranet sites. A briefing on the Privacy Management Plan will be incorporated in the PCO's induction program for new staff members.

## **Internal review procedures**

Internal review is a process where agencies handle complaints about how they have dealt with personal information. An aggrieved person can apply to the PCO for a review of conduct that he or she believes:

- breaches an information protection principle or a health privacy principle, or
- breaches a code of practice that applies to the PCO, or
- involves disclosure by the PCO of personal or health information kept in a public register.

Applications for internal review should be in writing and addressed to:

The Privacy Contact Officer  
Parliamentary Counsel's Office  
Level 23 AMP Centre  
50 Bridge Street  
Sydney NSW 2000

The Privacy Contact Officer will investigate the complaint concerning the way that the PCO has dealt with personal or health information. The PPIP Act provides that the review must be completed within 60 days of the date of receipt of the complaint by the agency. The Parliamentary Counsel will be responsible for the final determination of any internal review. The Parliamentary Counsel will notify the applicant and the Privacy Commissioner in writing of the outcome of any internal review. The Privacy Contact Officer will maintain a record of applications, reviews and outcomes.

The HRIP Act applies the provisions of the PPIP Act in relation to complaints and internal review procedures.

First issued June 2000.

Revised December 2004, December 2007 and January 2009.