

# Privacy Management Plan

Issued 2000/Revised June 2001/Revised 2003/Revised 2005

---

## Table of contents

### [Foreword](#)

### [1 Introduction](#)

- [1.1 Purpose](#)
- [1.2 The Privacy and Personal Information Act](#)

### [2 State Records](#)

- [2.1 The functions of State Records](#)
- [2.2 Duty of Confidentiality](#)
- [2.3 Policies, guidelines and procedures affecting privacy](#)

### [3 Implementing the Privacy Management Plan](#)

- [3.1 What personal information does State Records collect?](#)
- [3.2 What does an internal review involve?](#)
- [3.3 Compliance with the IPPs](#)
- [3.4 Compliance with the Public Register Provisions](#)

### [4 The Internal Review Process](#)

- [4.1 What do I do if believe my privacy has been breached?](#)
- [4.2 What does an internal review involve?](#)
- [4.3 How will I be informed of the outcome of an internal review?](#)

### [5 Staff Awareness](#)

### [Appendix 1](#)

### Browsable document

These procedures are also available as a [browsable document](#).

---

## Foreword

State Records welcomes the increased rights of the people of New South Wales to privacy and the Government's greater accountability in the way it creates and manages personal information. State Records takes seriously its role regarding the personal information that it collects and uses.

This Privacy Management Plan updates how State Records complies with the Information Protection Principles with its own records. The plan also outlines how State Records supports the principles through its role as the coordinating agency for standards of official recordkeeping in the NSW public sector under the *State Records Act 1998*. State Records pursues this role with an understanding of the importance of privacy and the way personal information in official records should be managed. State Records helps protect privacy by providing safe and secure storage for State records, promoting the timely disposal of records of temporary value, promoting high standards for official recordkeeping and by administering the framework for public access to State records more than 30 years old

The plan identifies State Records' responsibilities and policies that relate to the *Privacy and Personal Information Act 1998*. It also reflects the implementation of a program of actions that have further secured personal information collected by State Records since the issue of our first Privacy Management Plan. We will continue to review and improve upon these strategies and actions to ensure the plan remains a part of our everyday business.

David Roberts  
DIRECTOR

---

## 1 Introduction

### In this section

#### 1.1 [Purpose](#)

#### 1.2 [The Privacy and Personal Information Act](#)

- [1.2.1 What is personal information](#)
- [1.2.2 What are the Information Protection Principles?](#)
- [1.2.3 Privacy codes of practice](#)
- [1.2.4 Public registers](#)

#### 1.1 Purpose

The *Privacy and Personal Information Protection Act 1998* confers enforceable rights on the people of NSW in the way public sector agencies collect, store, use and disclose personal information. The Act protects personal information through 12 Information Protection Principles (IPPs). Under the legislation individuals have

the right to complain about the possible misuse of personal information through non-compliance with the IPPs.

The purpose of this management plan is to identify:

- the policies and strategies State Records will employ to comply with its obligations under the Act, and
- personal information collected and held by State Records.

The plan also details how these strategies and practises will be made known to staff and outlines the procedures for internal review when breaches of privacy are reported.

While this plan focuses on personal information collected and used by State Records, its roles as the coordinating agency for standards of official recordkeeping in the NSW public sector and as the custodian of many State records generated by other public sector agencies are also covered.

## **1.2 The Privacy and Personal Information Protection Act**

### **1.2.1 What is personal information?**

The Act defines personal information as:

Information or an opinion (including information or an opinion forming part of database and whether or not recorded in material form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion.

Personal information does not include information:

- contained in a publicly available publication
- about people who have been dead for more than 30 years, and
- about an individuals suitability for public sector employment.

The Act also allows for a number exceptions relating to law enforcement agencies.

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

The Act sets out the 12 Information Protection Principles (IPPs) in sections 8-19 of the Act. A brief summary of the IPPs is listed below. For a complete description please see the Act itself or *A Guide to the Information Protection Principles* published by Privacy NSW.

#### **1.2.2.1 Principle 1**

Collection of personal information must be for a lawful purpose that is directly related to a function of an agency and must be reasonably necessary.

#### **1.2.2.2 Principle 2**

Collection of personal information must be directly from the individual.

### **1.2.2.3 Principle 3**

When collecting personal information, the agency must make the individual aware of:

- the fact that the information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information
- whether the supply of information by the individual is required by law or is voluntary and any consequences for the individual if the information is not provided, and
- the existence of any right of access to, and correction of, the information.

### **1.2.2.4 Principle 4**

The agency must take reasonable steps to ensure that personal information collected is:

- relevant to the purpose
- not excessive
- accurate
- up to date, and
- complete.

### **1.2.2.5 Principle 5**

Personal information must be kept for no longer than is necessary for the purposes for which the information may be lawfully used, must be disposed of securely in accordance with any requirements for retention and disposal of personal information and must be protected against misuse.

### **1.2.2.6 Principle 6**

Information about personal information held by the agency should be accessible so as to allow individuals to ascertain whether it relates to them and, if so, the nature of the information, the purposes for which it is used and individual's entitlement to access the information.

### **1.2.2.7 Principle 7**

Personal information relating to an individual must be accessible to that individual without excessive delay or expense.

### **1.2.2.8 Principle 8**

The agency, on the request of an individual to whom the information relates, must amend personal information (through the correction, deletion or additions) to ensure that it is accurate, up to date, relevant, complete and not misleading.

### **1.2.2.9 Principle 9**

The agency must check the accuracy of personal information before use.

### **1.2.2.10 Principle 10**

Personal information should not be used for purposes other than for the purpose that it was collected unless the individual concerned consents, the new purpose relates to the old purpose, or it is used to prevent or lessen a threat to the life and health of any individual.

### **1.2.2.11 Principle 11**

The agency must not disclose personal information unless it directly relates to the purpose it was collected for, the person to whom it relates is reasonably aware that the disclosure usually occurs, or it is disclosed to prevent or lessen a threat to the life and health of any individual.

### **1.2.2.12 Principle 12**

The agency must not disclose information relating to ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities except to prevent death or injury. Personal information must not be disclosed to a jurisdiction outside NSW unless it has a privacy law approved by the Privacy Commissioner.

## **1.2.3 Privacy codes of practice**

Under the Privacy and Personal Information Protection Act, a privacy code of practice is a statement of how an agency proposes to depart from the Information Protection Principles or the public register provisions of the Act. A privacy code of practice can substitute for compliance with the IPPs.

## **1.2.4 Public registers**

A public sector agency that keeps a public register cannot disclose personal information except for the purposes for which the register exists. The Act also introduces a right enabling people to have personal details removed or hidden from view in certain circumstances.

---

## **2 State Records**

### **In this section**

#### **2.1 [The functions of State Records](#)**

- [2.1.1 Purpose](#)
- [2.1.2 Functions](#)

[Duty of confidentiality](#)

[Policies, guidelines and procedures affecting privacy](#)

## 2.1 The functions of State Records

To understand why State Records collects personal information and why it holds personal information it is necessary to detail its purpose and functions. These determine the personal information that State Records collects and uses. They also provide background for the roles that State Records plays as a coordinating agency of Government and as custodian of other agencies' records which may contain personal information.

State Records operates under the *State Records Act 1998*. The Act provides for the creation, management and protection of the records of public offices of the State and for public access to those records. It also establishes the State Records Authority of NSW and its Board.

### 2.1.1 Purpose

State Records' fundamental purpose is to ensure that the business of the NSW public sector is properly documented and the resulting records are managed efficiently and effectively for as long as they are needed, and that the State archives collection is developed preserved and used.

State Records is concerned with all aspects of recordkeeping, ranging from measures to ensure that public officials create records in the course of their duties in the first place, through the management of State records in public sector bodies, to preserving and making records of continuing value accessible as State archives.

State Records undertakes these roles variously as:

- a coordinating agency of Government
- a provider of services to the people and Government of New South Wales, and
- the protector and preserver of the State's official archives.

Most State records have a finite value and can be destroyed when this value has passed. Some, however, are preserved because they are of enduring value to the Government and/or to the community at large or to groups and individuals in it. Records of enduring value are called *archives* and State records transferred to our control as archives of the State are called *State archives*.

### 2.1.2 Functions

Section 66 of the State Records Act provides that State Records has the following functions:

- to develop and promote efficient and effective methods, procedures and systems for the creation, management, storage, disposal, preservation and use of State records
- to provide for the storage, preservation, management and provision of access to any records in its possession under the Act
- to advise on and foster preservation of the archival resources of the State, whether public or private
- to document and describe State archives in their functional and administrative context, and

- such other functions as are conferred or imposed on it by or under the Act or any other law.

State Records performs its functions by:

- setting and monitoring standards for the creation, management and disposal of State records
- providing practical advice, guidance and training to NSW public sector bodies in all aspects of records management
- providing centralised and cost-effective storage and retrieval services for the semi-active records of public sector agencies
- identifying those State records which should be retained as State archives and authorising the disposal of those which should not
- documenting and 'cataloguing' State archives in their functional and administrative context
- storing State archives in appropriate environments and ensuring that those stored elsewhere are also stored to the necessary standards
- using 'micro-' and 'macro-preservation' techniques to preserve the State's archives
- making State records more than 30 years old available for public access and use
- guiding public sector bodies in administering public access to those State records for which they are responsible
- interpreting, prompting and enhancing public awareness of the State archives collection, and
- making the best use of information technology and communications to improve our services and business.

## **2.2 Duty of confidentiality**

State Records' employees handle, have access to and inspect the records of other public sector bodies. This means that they regularly have access to records that contain personal information. The State Records Act recognises this and places a special duty of confidentiality on them (see Appendix 1).

## **2.3 Policies, guidelines and procedures affecting privacy**

In addition to the Privacy and Personal Information Protection Act, State Records is subject to other legislation and Government policy and procedures that help to ensure privacy is protected.

Legislation that has impact on the handling of personal information include:

- *Freedom of Information Act 1989*
- *Health Records and Information Privacy Act 2002*
- *ICAC Act 1988,*
- *Protected Disclosures Act 1994,* and
- *State Records Act 1998.*

The following policies and procedures of State Records also enable compliance with the Act:

- Code of Conduct
- Corporate Policy on Records Management

- Corporate Policy on Use of computer network
- Corporate Policy on Internal Communications
- Personnel Handbook
- Procedures for Making Access Directions (Procedures for Public Offices 3), and
- Procedures for Disposal Authorisation (Procedures for Public Offices 4).

The majority of professional staff at State Records are archivists and as such are subject to professional and ethical duties. These are set out in:

- Australian Society of Archivists' code of ethics, and the
- Australian Society of Archivists' privacy statement.

---

## 3 Implementing the Privacy Management Plan

### In this section

#### 3.1 [What personal information does State Records collect?](#)

- [3.1.1 Records relating to the provision of public access to State archives](#)
- [3.1.2 Records relating to corporate clients and suppliers](#)
- [3.1.3 Administration records](#)
- [3.1.4 Personnel records](#)

#### [Personal information in the custody of State Records](#)

- [3.2.1 Providing access to State records](#)
- [3.2.2 records in State Records' custody](#)

#### [Compliance with the IPPs](#)

- [3.3.1 Collection - principles 1 to 4](#)
- [3.3.2 retention and security - principle 5](#)
- [3.3.3 Notification, access and correction - principles 6 to 8](#)
- [3.3.4 Use - principles 9 to 10](#)
- [3.3.5 Disclosure - principles 11 to 12](#)

#### [Compliance with the Public Register Provisions](#)

### 3.1 What personal information does State Records collect?

State Records only collects personal information that relates to functions described in 2.1. This information primarily concerns the administration of personnel functions, providing access to State archives in an accountable way that ensures the preservation of the State's archival heritage and maintaining contact with clients and research and professional bodies.



### 3.1.1 Records relating to the provision of public access to State archives

#### 3.1.1.1 Information collected

State Records operates two reading rooms, one in Sydney and one in Western Sydney, where members of the public can view original State archives. Before individuals can access original records they are required to complete an **application for a readers ticket**. The application asks for name, address, and telephone contact. The information is collected directly from the individual. State Records requires individuals to show documentation that confirms their name, signature and address. Details of the documentation shown to confirm an individual's personal information are not recorded or kept.

The application is filled out in the reading room and the individual is informed on the application of the reasons for requesting the information, how the information will be used, their rights of access to the information and their rights to correct any inaccurate information.

The personal details are linked to a reader ticket number that tracks the issue of original records to the reading rooms.

Archives in Brief No. 13 *Reading room rules and procedures*, also details why personal information is collected. The Archives in Brief is available in State Records' reading rooms and on its Web site.

Members of the public also write to State Records with research and copying enquiries. These enquiries often contain not just the personal information details required for a reader's ticket, but sometimes they also contain personal information **volunteered in relation to an individual's genealogical heritage**. Such unsolicited information is defined in s. 4(5) of the Privacy and Personal Information Protection Act as not 'collected'.

Overt **closed circuit television** (CCTV) is installed in the public areas at the Western Sydney Records Centre and the Sydney Records Centre. The cameras are visible and the public is notified of the use of CCTV through prominent signage. They operate between the hours of 9 am and 5pm. A monitor displays images from the cameras in staff areas. The cameras were installed in compliance with the code of practice for the Use of Overt Video Surveillance in the Workplace

#### 3.1.1.2 Purpose of collecting the information

**Protecting the State archives:** the reader ticket number tracks the issue of records to the reading rooms. Collecting contact details enables State Records to follow up with the reader if any problems, such as damage or theft, are identified. The use of CCTV protects records, exhibition material and property by providing a deterrent from potential damage and theft and by allowing on the spot policing through the use of monitors and capturing evidence in the event of theft or damage occurring.

**Understanding uses of the State archives:** collecting information on type of research helps State Records to plan and allocate resources more effectively by monitoring interest in different parts of the collection.

### **3.1.1.3 Storage, security and disposal of personal information**

Reader's ticket application forms are kept for 5 years before being destroyed under an approved disposal authority. The originals are kept, in an area accessible only by staff, for 12 months and then transferred to the Western Sydney repository before destruction.

The information is also entered into a database located on a secure network. Only appropriate staff with an authorised password can access the database.

State Records files requests for research on reference files and stores them in secure storage. Files on routine requests are destroyed after 5 years under an approved disposal authority.

CCTV tapes from the cameras are stored in secure storage accessible by only authorised staff. They are held for 3 months and then reused.

## **3.1.2 Records relating to corporate clients and suppliers**

### **3.1.2.1 Information collected**

State Records supplies services to a wide range of NSW public sector bodies and other organisations and purchases goods and services from many suppliers. Personal information collected for contacts in these organisations is restricted to normal work contact, such as position title, telephone and fax numbers and e-mail address. This information is collected directly from the individual, from published sources or from the organisation concerned.

The supply of State Records' goods and services also requires the collection of personal information. Client details such as name, address and credit card number are often supplied when purchasing publications or services such as seminars and copies of State archives.

### **3.1.2.2 Purpose of collecting the information**

State Records collects the information as part of legal obligations, for invoicing/billing and delivery.

### **3.1.2.3 Storage, security and disposal of personal information**

The information held on files is kept in secure storage and the information held in databases is only accessible to authorised staff. The information is not used for any other purpose and is not released outside State Records. The information is destroyed or deleted under authorised disposal authorities, notably *General Disposal Authority 7: Financial and Accounting Records*, when no longer required.

## **3.1.3 Administration records**

### **3.1.3.1 Information collected**

State Records is currently in the process of rationalising its **contact lists** into a single database. When completed, the database will contain contact information for:

- recipients of State Records' magazine and newsletters
- chief executives, corporate records managers and other key contacts in NSW public sector bodies
- office holders in professional bodies, research and community groups relevant to State Records' functions and services
- contacts in regional repositories, community access points and other holders of the Archives Resources Kit, and
- contacts in other archives institutions and similar organisations.

The information that makes up the contact databases is either collected directly from the individual or from publicly available sources.

State Records maintains contact details of members of its **Board and advisory committees**. Information about Board members includes private as well as work contact details.

### ***3.1.3.2 Purpose of collecting the information***

Contact list information is collected to enable State Records to distribute news and other information connected with its functions and to correspond with relevant people and organisations.

Contact details of members of the Board and advisory committees is used to support the administration of meetings. Private contact details of Board members are collected to enable them to be contacted in urgent cases or emergencies.

### ***3.1.3.3 Storage, security and disposal of personal information***

The database is accessible to all network users but only modified by a restricted number of authorised users. The information is kept as long as it is relevant, is updated when necessary and deleted when no longer required.

Contact details of Board members are held securely and are accessible only to the Director and Associate Director, City (secretary to the Board).

## **3.1.4 Personnel records**

### ***3.1.4.1 Information collected***

State Records maintains information detailing home address and telephone number, any medical conditions of staff (if disclosed voluntarily) and next of kin details to be used in cases of emergency. Also maintained are details of all leave taken, information on each employee's substantive and acting work and salary history; and details of qualifications submitted by the employee, together with a record of all internal and external training courses undertaken. These details are disclosed to other staff only on an as-needed basis and only for business or health and safety purposes. All staff are made aware of the existence of this information and the purposes for which it is used.

State Records also maintains attendance and performance management system records and, where relevant, records relating to disciplinary processes, medical matters and workers compensation. All such records are created and maintained in accordance with the requirements of the Personnel Handbook and of relevant legislation.

The *curriculum vitae* and resumés of applicants and/or preferred candidates are used to assist the recruitment process of staff.

From time to time individuals forward their *curriculum vitae* and resumés to State Records seeking work opportunities. This information is maintained on file and individuals are informed of this action.

State Records outsources its payroll function to the Central Corporate Services Unit (CCSU), a business unit of the Department of Commerce, and does not keep payroll records relating to employees.

#### **3.1.4.2 Purpose of collecting the information**

The collection of personal information is essential for State Records in administrating human resources, financial services, office services and recruitment.

#### **3.1.4.3 Storage, security and disposal of personal information**

The files holding this information are subject to strict security and are only accessible by authorised staff. Personal information held in databases is accessible only to authorised staff and can only be altered by the Human Resources Officer. Personnel records are disposed of in accordance with *General Disposal Authority 3: Personnel Records*.

### **3.2 Personal information in the custody of State Records**

As part of its functions, State Records has custody of the records of other public offices. These records can be divided into two categories:

- records transferred to State Records as State archives, and
- records stored in the Government Records Repository.

Both categories can contain personal information.

#### **3.2.1 Providing access to State records**

Section 51 of the State Records Act requires public offices to make access directions in relation to the records more than 30 years old for which they are responsible, including those held by State Records as State archives, that either to open or to close them to public access.

Access directions are based on the known or likely contents of a series, group or class of records. The Attorney General has issued guidelines on *Making Access Directions under Part 6 of the State Records Act 1998*, under s. 52(3) of the Act. The guidelines are intended to promote consistency in the making of access directions by identifying the types of information in a record series or class that may make them open or closed to public access after 30 years. They address issues such as personal information, privacy, passage of time, security and confidentiality. Passage of time is an important issue when decisions are made to make State records available for public access. As noted in 1.2.1 personal information does not include information relating to an individual who has been dead for 30 years. The guidelines do, however, identify types of sensitive personal information that should not be released to public access about deceased individuals until a suitable passage time.

State Records ensures that records transferred to its custody as State archives are made available to the public only in accordance with the relevant access direction. State Records monitors access directions to assist in identifying and rectifying any inconsistencies, including access directions to records containing personal information.

Access to records closed to public access is at the discretion of the responsible public office. State Records does not facilitate such access unless that access has been properly authorised, for example, under the 'special access' provisions (s. 58) of the Act.

### **3.2.2 Records in State Records' custody**

Under s. 4(4) of the Privacy and Personal Information Protection Act, information contained in records in State Records' custody is defined as 'held' by the public sector agency responsible for the records, not by State Records.

Nonetheless, State Records helps protect personal information in such records. Both categories of records noted above are held in secure environments at the Western Sydney Records Centre and, in much smaller quantity, at the Sydney Records Centre. Only authorised staff have access to the records.

## **3.3 Compliance with the IPPs**

### **3.3.1 Collection - principles 1 to 4**

State Records collects all personal information directly from the individual except in some cases when compiling information for public sector contacts. When not collected directly from the individual, the information is collected from publicly available sources such as the Government Directory and telephone books.

Public clients are made aware the information is being collected and why it is collected by information on the application for a reader's ticket and in the rules and procedures for the reading rooms. Address and contact information is collected only from readers who wish to use original records. Clients are informed of the use of CCTV through prominent signage in the public areas at both record centres.

### **3.3.2 Retention and security - principle 5**

The database containing the personal information of public clients issued with readers' tickets is on a secure location on the computer network and access is restricted to authorised staff. The tapes of CCTV monitoring are held in a secure storage accessible by only authorised staff and the information erased through the reuse of the tapes every 3 months.

### **3.3.3 Notification, access and correction - principles 6 to 8**

As State Records collects most personal information directly from the individual, it is reasonable to assume that individual is aware that the information is held by State Records and that the information is accurate at the time it is collected. State Records alerts clients of the existence of the information by publishing the Privacy Management Plan on its Web site and by making it available in its two reading rooms.

State Records encourages individuals to advise of any change in personal information they have supplied. State Records alerts public clients of their rights of access to this information on the reader's ticket application form and also of their rights in relation to alteration of the information.

### **3.3.4 Use - principles 9 to 10**

State Records does not use personal information for a purpose other than for the reason it was collected unless the individual concerned consents, the new purpose relates to the original purpose, to prevent death and illness or it is otherwise permitted under an exemption under the Act. The use of personal information within State Records is governed by policies and guidelines listed in 2.3.

### **3.3.5 Disclosure - principles 11 to 12**

State Records does not disclose personal information, including the ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless it is to prevent a threat to the life or health an individual, and unless otherwise exempted under the Act.

## **3.3 Compliance with the Public Register Provisions**

State Records is responsible for the public register of access directions. The register details the title and description and location of records covered by an access direction. If an access direction closes records to public access the register also details why the records are closed and for how long. The register does not contain personal information.

---

## **4 The Internal Review Process**

### **In this section**

[What do I do if I believe my privacy has been breached?](#)

[What does an internal review involve?](#)

[How will I be informed of the outcome of an internal review?](#)

### **4.1 What do I do if I believe my privacy has been breached?**

If an individual has a complaint about the conduct of State Records or a member of its staff in relation to the collection, storage, use or disclosure of personal information, a written request should be sent (on paper or by e-mail) to State Records so that an internal review may be undertaken. An application for an internal review can address a breach in the IPPs, a privacy code or the improper disclosure of personal information from a public register.

Under s. 53(3) of the Privacy and Personal Information Protection Act, an application for an internal review must:

- be in writing
- be addressed to State Records
- specify an address in Australia to which a notice may be sent
- be lodged with State Records within six months (or such later date as State Records may allow) from the time the applicant first became aware of the conduct the subject of the application, and
- comply with such other requirements as may be prescribed by the regulations to the Act.

## **4.2 What does an internal review involve?**

An application for internal review will be dealt with by an employee of State Records who has the authority of the Director to deal with the matter. The employee will not have been substantially involved in the matter that is the subject of the application. This will normally be the Chief Information Officer.

The review will be completed as soon as is reasonably practicable in the circumstances and within 60 days from the day on which the application was received.

As a result of the review State Records may:

- take no further action on the matter; or
- make a formal apology to the applicant; and/or
- take such remedial action as thought appropriate; and/or
- provide undertakings that the conduct will not occur again; and/or
- implement administrative measures to ensure that the conduct will not occur again.

State Records is required to:

- notify the NSW Privacy Commissioner of an application for internal review
- provide reports to the Privacy Commissioner on the progress of the internal review
- inform the Privacy Commissioner of the findings of the review and of the action to be taken by State Records in relation to the matter.

If requested by State Records, the Privacy Commissioner may undertake the internal review.

## **4.3 How will I be informed of the outcome of an internal review?**

State Records will acknowledge the receipt of an application and write to an applicant within 14 days after completing the review and advise the applicant of:

- the findings of the review (and the reasons for those findings)
- action proposed to be taken (and the reasons for taking that action), and
- the right of the applicant to have the findings, and State Records' proposed action, reviewed by the Administrative Decisions Tribunal in NSW.

---

## 5 Staff awareness

Staff have been notified of this plan through the staff newsletter. The plan is available to staff on the corporate intranet.

All staff have been encouraged to undertake the Privacy Training Module available on State Records intranet.

The following resources are part of the Induction Manual and given to all new staff :

Privacy NSW Fact Sheet No 2:

[http://www.lawlink.nsw.gov.au/pc.nsf/files/FS2\\_ipps.pdf/\\$FILE/FS2\\_ipps.pdf](http://www.lawlink.nsw.gov.au/pc.nsf/files/FS2_ipps.pdf/$FILE/FS2_ipps.pdf)

Privacy Management Plan on the Web site:

<http://www.records.nsw.gov.au/about/privacyplan/privacytoc.htm>

Privacy training module on the intranet

---

## Appendix 1

Section 73 of the State Records Act states:

(1) A person who acquires information in the exercise of functions under this Act must not directly or indirectly make a record of the information or divulge it to another person except in the exercise of functions under this Act.

(2) It is not an offence under subsection (1) if, in legal proceedings, a person:

- (a) discloses information in answer to a question that the person is compellable to answer, or
- (b) produces a document or other thing that the person is compellable to produce.

(3) The provisions of any other Act imposing restrictions or obligations on a person as to secrecy or disclosure of information acquired in the course of the administration of that Act extend to apply to a person who, in the exercise of functions under this Act, gains access to that information as a result of the information having been acquired in the course of the administration of the other Act. For that purpose the person who gains access to the information in the course of the administration of this Act taken to be a person engaged in the administration of the other Act.

(4) This section does not prevent or otherwise affect:

- (a) the giving of access to records under Part 6 (Public access to State records after 30 years), or
- (b) the preparation and dissemination of guides and finding aids.

(5) This section does not apply to the divulging of information to, or to the production of any document or other thing to, any of the following:



- (a) the Independent Commission Against Corruption,
  - (b) the National Crime Authority,
  - (c) the New South Wales Crime Commission,
  - (d) the Ombudsman,
  - (e) any other person prescribed for the purposes of this section.
- 

**State Records Authority of New South Wales Sydney, Australia**

**First edition August 2000. Revised edition June 2001. Revised November 2003. Revised 2005**

**© Copyright reserved by the Government of NSW, 2005. All rights reserved. No part of this publication may be reproduced by any method without the prior written consent of the State Records Authority of NSW.**

**ISBN 0-7313-9721-5**