

Department of State and Regional Development

PRIVACY MANAGEMENT PLAN

Version 2

Version Control

Title: DSRD – Privacy Management Plan

Subject: Privacy

Responsible: Business Governance Unit

Authorised: Executive Director, Policy and Resources

Publication Date: 27th August 2004

Version: 2.0

Review Date: Every three years

Distributed to: Every individual engaged by the Department as a permanent officer, under employment contract, term appointment (including secondment), or temporary arrangement.

CONTENTS

	Pages
Introduction	3 - 6
Personal Information	
Application of the Plan	
The Department	
• clients	
• employees	
• contractors and consultants	
Outsourced Service Providers	
Public Registers	
Part 1	6-18
Policies and Implementation Strategies for Compliance	
Collection	
Storage	
Access and Accuracy	
Use	
Disclosure	
Identifiers & Anonymity	
Transferrals & Linkage	
Part 2	18-19
Dissemination of Privacy Policies	
Part 3	19-20
Other Relevant Matters	
Privacy codes of practice	
Contracts with third party contractors/consultants	
Confidentiality and commercial in confidence	
Regular review of the collection, storage and use of personal information	
Regular review of the Privacy Management Plan	
Part 4	21-22
Procedures for Conducting Internal Reviews	
Appendix 1 – Application Form for Internal Review	23-24

Introduction

The Privacy Management Plan outlines the Department of State and Regional Development's information handling policies and practices designed to maximise compliance with the principles and requirements of the *Privacy and Personal Information Protection Act 1988 (NSW)* ("PPIP Act") and the *Health Records Information Privacy Act 2002 (NSW)* ("HRIP Act"). Both Acts are referred to in the Plan as the "Privacy Acts".

The Privacy Acts provide for the protection of personal information and health information, and for the protection of the privacy of individuals by means of information protection principles. These principles cover the collection, storage, use and disclosure of personal and health information. The Privacy Acts also contain a number of exemptions to the operation of these principles. A summary of the information protection principles and the exemptions and how the Department will comply with the principles in its operations is provided in Part 1 of this Plan.

The Department will continue to make the Plan available to all its employees and clients, and the community generally.

Nothing in the Plan is to affect:

- any matter of interpretation of the information protection principles as they apply to the Department;
- any obligation at law cast upon the Department by way of representation or holding out in any manner whatsoever; and
- create, extend or lessen any obligation at law which the Department may have.

For the purposes of the Plan, a reference to 'personal information' includes both personal information and health information, unless otherwise specified.

Personal information

"Personal information" is any information or opinion about a person whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes records in a material form (e.g., written files, databases) containing a person's name, address, sex, etc., or physical information like fingerprints, retina prints, body samples or genetic characteristics. Personal information does not necessarily have to be recorded on a database or be in a material form. Personal information could include written records about a person, a photograph or image of a person, fingerprints or DNA samples that identify a person, or information about a person that is not written down, but which is in the possession or control of the agency.

"Health information" is a specific type of personal information. Health information includes personal information that is information or an opinion about the physical or mental health or 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.

Version 2.0

Publication Date: 27th August 2004

Authorised: Executive Director, Policy and Resources

Review Date: Every three (3) years

The Department collects, stores and uses much information. Only a small part of that information is personal information covered by the Privacy Acts. The remainder may be classed as business information. This Plan only applies to that part of the Department's information that is personal information. However, where personal information cannot be meaningfully separated from business information, this may mean that business information may receive treatment of a higher standard, namely, treatment accorded to personal information.

What personal information is not covered by the Privacy Acts?

Personal information does not include information about an individual that is contained in a publicly available publication. Personal information, once it is contained in a publicly available publication (e.g., telephone directory), ceases to be covered by the Privacy Acts. However, if personal information from a published source is copied into DSRD's records (e.g., client mailing lists), that personal information is then covered by the Privacy Acts.

What personal information is exempt from the Privacy Acts?

Personal information commonly exempt from both Privacy Acts includes:

- information about an individual who has been dead for more than 30 years
- information about individuals contained in publicly available publications
- information contained in a protected disclosure, or collected in the course of investigating a protected disclosure
- information arising from Royal Commissions or special commissions of inquiry
- information in Cabinet documents and Executive Council documents
- a number of classes of information which relate to law enforcement activities such as telephone interception, witness protection programs and the investigation of complaints about police officers
- information about a person's suitability for public sector employment i.e., job applications, references, service reports and pre-employment criminal record checks, but probably not an individual's subsequent employment records.

Health information specifically exempt from the HRIP Act includes:

- information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition
- information about an individual that is contained in a State record under the control of the State Records Authority that is available for public inspection in accordance with the *State Records Act 1998*
- information about an individual that is contained in archives within the meaning of the *Copyright Act 1968* of the Commonwealth
- information about an individual that forms part of an employee record (within the meaning of the *Privacy Act 1988* of the Commonwealth) about the individual held by a private sector person
- information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection.

Application of the Plan

The Plan applies, wherever practicable, to:

- Departmental clients
- Departmental employees
- contractors and consultants engaged by the Department, as follows:

Clients

In accordance with the *State Development and Industries Act 1966 (NSW)* and other legislation administered by the Department, the Department's aim is to advance the economic development of New South Wales and bring new business into the State. In line with its stated aims and objectives, the Department's clients are companies, registered and unregistered businesses, sole traders and farmers.

The Department needs to collect personal information from clients to enable it to provide and improve its services to clients.

Generally, there is no business reason for the Department to collect and store health information in relation to our clients. However, there may be occasions where health information about a client is collected, e.g., a client's disability may be noted, if it affects his/her ability to access our services.

The Department will treat all personal information collected from clients in accordance with the information protection principles of the Privacy Acts.

Employees

Personal information gathered by the Department about its employees includes:

- recruitment material (except information or an opinion about an individual's suitability for appointment or employment as a public sector official)
- leave and payroll data
- personal contact information
- performance management plans (except where the material may form the basis of a disciplinary matter)
- complaints by clients
- wage and salary entitlements.

Other personal information may include health information gathered at the time of recruitment e.g., disability information requiring workplace adjustments, or information collected during employment e.g., workplace injuries or illnesses for workers compensation purposes and sick leave applications.

All personal information is held by the Department's Human Resources Unit and, in some cases, the Central Corporate Services Unit (CCSU) as the Department's outsourced provider of human resource management services e.g., payroll, leave management.

The Department will treat all personal information collected from its employees in accordance with the information protection principles of the Privacy Acts.

Contractors and Consultants

The Department engages contractors and consultants for the performance of a number of services. These third party contractors must abide by the information protection principles of the Privacy Acts under the terms of their engagement with the Department.

The Department may also provide tied funding to client businesses to employ consultants or may provide a list of suitability qualified consultants, in a given field of expertise, to client businesses for the purpose of employing the consultant to improve

the functioning of that client business. These consultants must also abide by the Privacy Acts.

Outsourced Service Providers

The Department has contractual arrangements with a range of service providers to deliver services on its behalf. These contracts are ongoing and in some cases span a number of years. Some of these were in existence prior to the Act. Existing contracts are being reviewed to reflect the obligations of the Department under the Act. New contracts will include appropriate clauses covering compliance issues.

Public Registers

The Department keeps no public registers.

Part 1 Policies and Implementation Strategies for Compliance

This part of the Plan considers the Department's policies and strategies for handling personal information in accordance with the information protection principles defined in the Privacy Acts. These principles describe what the Department must do when it collects, holds, stores, uses and discloses personal information. These principles can be grouped into seven categories: collection, storage, access and accuracy, use, disclosure, identifiers and anonymity, and transferrals and linkage.

The Department's policies and implementation strategies relating to these principles and any relevant exemption that modifies these principles are stated in this section.

Note: a reference to 'personal information' includes both personal information and health information, unless otherwise specified.

COLLECTION

Lawful - *When an agency collects personal information, the information must be collected for a lawful purpose. It must also be directly related to the agency's activities and be necessary for that purpose.*

The Department's Policy and Implementation Strategy

The Department will only collect personal information for a lawful purpose which directly relates to its function. The Department will not collect any more information than is necessary for it to fulfil those functions. Anyone engaged to collect information for the Department will be required to comply with the Privacy Acts as part of their terms of engagement.

Prior to any formal use, any information collection forms or other mechanisms designed to collect personal information must be referred to the Department's Privacy Contact Officer or relevant Divisional Privacy Resource Officer, for advice as to:

- whether the personal information is collected for a lawful purpose
- if that lawful purpose is directly related to a function of the Department
- whether or not the collection of that information is reasonably necessary for the specified purpose.

The Department will continue to monitor and review the effectiveness of the privacy statements it includes on all information collection forms and actively ensure that staff are aware of the Department's privacy obligations, strategies, policies and procedures.

***Direct** - Personal information must be collected directly from the person to whom it relates unless that person has authorised collection from someone else or the person is under the age of 16 and the information has been collected from the person's parent or guardian. More specifically, health information must be collected directly from the person to whom it relates, unless it is unreasonable or impracticable for the organisation to do so.*

The Department's Policy and Implementation Strategy

The Department will only collect information directly from an individual to whom the information relates, unless the individual has authorised collection of the information by someone else or in the case of health information, where it is unreasonable or impracticable to do so. Personal information relating to a person under the age of 16, may also be collected from their parent or guardian.

The following outlines the practices for the collection of personal information implemented by the Department to ensure compliance with the Privacy Acts.

A. Applications by clients for assistance or services

During the process of applying for assistance from the Department, personal information is provided directly by the individual or applicant seeking assistance. The Department will check the accuracy, completeness and the currency of this information by obtaining information directly from the applicant.

B Agency agreements

The Department has various agreements with outsourced service providers to deliver services on behalf of the Department. These providers include Small Business Advisory Centres, Innovation Advisory Centres, and Regional Development Boards. It is the responsibility of these providers under their agreements with the Department, to obtain the authority from the client for the indirect collection of personal information.

C Collection of personal information by consultants

The Department provides tied funding to client businesses for the purpose of obtaining various kinds of consultancy services. In these circumstances, the Department collects information or feedback indirectly from the client businesses concerning the quality of the services provided by the consultant in the provision of the consultancy services. As a pre-condition to being placed on the Department's *Eligible Consultants Register*, each consultant provides their authority for the indirect collection of personal information by the Department from the client business who received the consultant's service.

D. Forums

During the course of exercising its proper functions, the Department funds, sponsors or co-sponsors many forums or special events, both nationally and inter-nationally. From these forums or special events the Department receives a list of participants or

Version 2.0

Publication Date: 27th August 2004

Authorised: Executive Director, Policy and Resources

Review Date: Every three (3) years

delegates who attended these events. The Department will endeavour to ensure that these individuals have authorised any indirect collection of their personal information. The Department then incorporates these lists into its consolidated database of contact names and details.

E. Employees

The Department collects personal information directly from its employees to administer staffing matters and provide human resource management services to its employees.

The Central Corporate Services Unit (CCSU) will also be collecting some of the same personal information on behalf of the Department directly from employees. This Plan applies only to those practices conducted by the Department. The functions which are carried out by the CCSU are not the subject of this Plan.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- if the information collected is connected with proceedings before a court, tribunal, royal commission, coronial inquiry (whether or not actually commenced)
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency
- law enforcement and investigative agencies where compliance might interfere with law enforcement or investigative functions
- where compliance would prejudice the interest of the individual to whom the information relates
- where non-compliance is “necessarily implied” or “reasonably contemplated” under any Act or law.

Statutory exemptions from the HRIP Act apply:

- if the information collected, held, managed, used, disclosed or transferred is in connection with his or her personal, family or household affairs
- if the information collected, used, held or disclosed is connected with news media activities.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Open - *When personal information is collected reasonable steps must be taken to ensure that the person to whom it relates is aware of:*

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

The Department's Policy and Implementation Strategy

The Department will provide a privacy statement or notification, wherever possible, which notifies persons of the matters raised above. Similarly, any consultant, contractor or other third party engaged by the Department which may be involved in the collection of personal information will also be required to provide such a notification to any person from whom information is collected.

The Department cannot always ensure that information collected by a forum or event convener will comply with the requirements of this principle. However, wherever possible, contractual requirements will be put in place to effect compliance.

The Department's websites cater for the information needs of a diverse group of industries, specific target client groups as well as small businesses. The Department has a standard privacy statement available from its websites. The Department has appropriate privacy statements on its information collection forms, brochures and other publications.

At the point of the collection of personal information from an employee to whom the information relates, the Department will provide privacy notification as required by this principle. The CCSU will also be collecting some personal information from employees. This Plan applies only to the Department's practices and not the functions or processes of CCSU.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where information is collected for law enforcement purposes
- an investigative agency where compliance might interfere with investigative functions
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency
- where an agency is authorised or required not to comply under any Act or law
- where non compliance is "necessarily implied" or "reasonably contemplated" under any Act or law
- where compliance would prejudice the interest of the individual to whom the information relates
- where the individual expressly consents.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Relevant – *An agency will ensure that personal information collected is relevant, accurate, up to date and not excessive. The collection should not unreasonably intrude into the personal affairs of the individual.*

The Department's Policy and Implementation Strategy

The Department will comply with this principle having regard to the purposes for which the information is collected. While implementing this principle, there may be limited circumstances when an amount of financial and/or non-financial assistance is given, or proposed to be given, to a client creates such a compelling public interest to ensure that the assistance is given to a client who is capable of competently utilising the assistance. For such cases, the Department has developed a privacy notification and consent provision to enable the Department to make enquiries pertaining to

competencies of key operational persons within the client company. The legislative basis for the granting of financial assistance is contained in Section 20 (3) of the *State Development and Industries Assistance Act 1966 (NSW)*. The Department reserves its right to determine the conditions that must be met to satisfy the public interest in the granting of substantial amounts of financial assistance.

STORAGE

Secure – *Personal information must be stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected from unauthorised access, use or disclosure.*

The Department's Policy and Implementation Strategy

The Department will ensure that information is held no longer than necessary. The Department will dispose of information securely and in accordance with its relevant records management policies and procedures.

Any information collected will be protected against loss, unauthorised access, use, modification or disclosure, and against other misuse. When information must be given to a person in connection with the provision of a service to the Department, the Department will endeavour to prevent unauthorised use or disclosure of the information.

Where information is given to a person or agency outside the Department or collected by a third party for the provision of a service to the Department or a client of the Department, the Department will seek to oblige that third party to comply with the information protection principles by contract.

This policy and strategy should be read in conjunction with the Department's policies and procedures for records management and for use of its communication and information technology (C&IT) devices.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where an agency is authorised or required not to comply under any Act or law
- where non compliance is "necessarily implied" or "reasonably contemplated" under any Act or law
- law enforcement and investigative agencies where compliance might interfere with law enforcement or investigative functions.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Access & Accuracy

Transparent – *An agency must provide individuals with enough details about what personal information it is storing about them, why the agency is storing it, and what rights individuals have to access it.*

The Department's Policy and Implementation Strategy

The basic purpose of this principle is to allow individuals to know whether the Department holds information about them. The Department promotes its newsletters,

business information brochures, events and workshops and various programs of assistance through the internet and includes a privacy statement on its websites. This is a relative principle and as a matter of practicality, not every item of personal information will be capable of ascertainment by the Department.

The Department will take reasonable steps to enable a person to determine whether it holds personal information about them, subject to the provisions of the *Freedom of Information Act 1989 (NSW)* ("FOI Act"). If the Department holds any personal information about a person, upon request it will advise them the nature of that information, the main purposes for which it is held, and that person's entitlement to access.

Where an application is received, the Department will institute a search of the records where it is likely that personal information would be held by the Department. The Department may ask the applicant to describe what dealings the applicant has had with the Department in order to assist the search. The Department will ordinarily provide a response to applications of this kind within 21 days of the application being made. The fee structure is commensurate to that of the Department's FOI Act rates structure.

General inquiries concerning the personal information that is held by the Department are to be directed to the Privacy Contact Officer who can be contacted on (02) 9228 4622.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where an agency is authorised or required not to comply under any Act or law
- where non compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Accessible – *An agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.*

The Department's Policy and Implementation Strategy

Where the Department holds information about an individual it will allow that person to access their own personal information. Upon request by any person, the Department will give access to that person to personal information held about them, subject to the provisions of the FOI Act. If the Department holds any information about a person, upon request it will advise them of the nature of that information, the main purposes for which it is held, and that person's entitlement to access.

Where an application is received, then the Department will institute a search of the records where it is likely that personal information would be held by the Department. The Department may ask the applicant to describe what dealings the applicant has had with the Department in order to assist the search. The Department will ordinarily provide a response to applications of this kind within 21 days of the application being made. The fee structure is commensurate to that of the Department's FOI Act rates structure.

General inquiries concerning the personal information that is held by the Department are to be directed to the Privacy Contact Officer who can be contacted on (02) 9228 4622.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where an agency is authorised or required not to comply under any Act or law
- where non compliance is “necessarily implied” or “reasonably contemplated” under any Act or law.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Correct – *When an agency holds information about a person it must, at the request of the person, make appropriate amendments to ensure the information is accurate, up to date, relevant, complete and not misleading.*

The Department’s Policy and Implementation Strategy

The Department seeks to ensure that all the personal information it holds is current and accurate and complete. The Department will, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions).

A request to amend information must be in writing by the individual to whom the information relates. Where information amendments are requested, this will be undertaken as soon as reasonably practicable.

The Department collects a variety of personal information. The bulk of the personal information is contained in the Department’s databases. This personal information is purely “contact details” containing mainly company names, addresses, and telephone numbers. However, these databases may also contain some personal information in the form of personal names and job titles for those persons. Where a person wishes to alter their personal information on the Department’s database, the Department will accept an oral request to amend the personal information.

Where a person requests an amendment to personal information, and where that personal information is not merely a contact detail, the Department may require further documentary evidence to support amendments. Depending on the nature of the amendment requested, the Department may require the person to complete a statutory declaration. Where the Department makes a request for a statutory declaration, that declaration should be accompanied by appropriate evidence.

Where the Department is not prepared to amend

If the Department is not prepared to amend the personal information in accordance with a request by the individual, the Department may attach to the information in such a manner as is capable of being read with the information, any statement provided by that individual.

Where an amendment is made

If personal information is amended, the individual to whom the information relates is entitled, if it is reasonably practicable, to have the recipients of that information

notified of the amendments made by the Department.

State Records Act 1998

The State Records Act 1998 generally does not allow for the deletion of a state record. By section 20(4) of the PPIP Act, some deletions may be allowed in accordance with the discretion of the Department's Director General. It may be necessary to obtain legal advice for specific cases.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where an agency is authorised or required not to comply under any Act or law
- where non compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Accurate - *An agency must take reasonable steps to ensure that an individual's personal information is relevant, accurate, up to date, complete and not misleading before using it.*

The Department's Policy and Implementation Strategy

Wherever it appears that personal information may be used or disclosed, and having regard to the purpose for which the information is to be used, a check of the currency of that information will be necessary. The significance of the information will assist the Department to determine whether it checks each and every item of personal information.

It is not possible to say in advance when such checks should be taken. It will depend on the age of the information, its likelihood of change and the particular function for which the information was collected. For example, in a process for obtaining the Department's assistance, once the determination process is complete, the personal information is no longer required and can be stored or disposed of securely in accordance with the Department's records management policies and procedures.

USE

Limited – *An agency must not use personal information other than for the purpose for which it was collected unless:*

- *the person who is the subject of the information consents*
- *the other purpose is directly related to the original purpose*
- *the use of the information for the other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of another person.*

The Department's Policy and Implementation Strategy

The Department uses personal information for promotional purposes integral to its statutory promotional functions. Where the Department has entered into a co-operative agreement or a partnership with a third party that involves a joint promotional activity, it will seek to contractually bind each party to comply with the

principle, and to limit the use of the personal information solely for the purpose of that promotional activity.

Where personal information collected for one purpose by or on behalf of the Department is to be used for another purpose, the person will be requested to provide their consent to the use of the information for that other purpose.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where the use is reasonably necessary for law enforcement purposes or the protection of public revenue
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency
- where an agency is authorised or required not to comply under any Act or law
- where non compliance is “necessarily implied” or “reasonably contemplated” under any Act or law
- where a disclosure is required to be made to the Minister for the purpose of informing the Minister about any matter within the Minister’s administration.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

DISCLOSURE

Restricted/Limited – *An agency must not disclose personal information to another body, including another public sector agency, unless:*

- *the purpose of the disclosure is directly related to the purpose for which the information was collected*
- *the person concerned is reasonably likely to be aware, or has been made aware, that information of that kind is usually disclosed to the body, or*
- *the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person concerned.*

The Department’s Policy and Implementation Strategy

The Department may disclose personal information to another person or other body where this disclosure is directly related to the purpose for which the personal information was collected and the individual concerned is reasonably likely to have been aware of the intended recipients of that information.

“Directly related” can mean the disclosure to another person or agency to deliver a service which supplements that of the Department or disclosure to a person or agency for the purpose of assessing or reviewing the delivery of a program to which the original collection relates.

Where the Department collects personal information for one purpose and then needs to use the personal information for another purpose, the Department must first obtain the consent of the individual to whom the information relates.

Section 16 of the *Small Business Development Corporation Act 1984 (NSW)* and section 12 of the *Country Industries (Pay-Roll Tax Rebates) Act 1977 (NSW)* may also have the effect of placing a dual responsibility on the Department not to disclose information or personal information obtained in performance of functions under these

Acts. Whether the requirements of these Acts apply will depend upon the nature of a particular matter. It may be necessary to obtain legal advice if any of the compliance obligations are to be relied upon or clarification about interaction with the Privacy Acts is required.

The Department will comply with the Premier's Department Circular No. 2003-50 concerning "*Privacy Guidelines on Disclosure of Information During Industrial Relations Consultations*". The Guidelines recognise that Industrial Relations legislation and Occupational Health and Safety legislation may require personal information to be disclosed in certain circumstances.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where disclosure is made in connection with proceedings for an offence or for law enforcement purposes
- where disclosure is made to a law enforcement agency for the purpose of ascertaining the whereabouts of a person reported to be missing
- where disclosure is authorised by subpoena, search warrant or other statutory instrument
- where the use is reasonably necessary for law enforcement purposes or the protection of public revenue
- where disclosure is reasonably necessary to investigate an offence where there are reasonable grounds to believe an offence has been committed
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency
- where an agency is authorised or required not to comply under any Act or law
- where non compliance is "necessarily implied" or "reasonably contemplated" under any Act or law
- where the person expressly consents
- where a disclosure is required to be made to the Minister for the purpose of informing the Minister about any matter within the Minister's administration.

Statutory exemptions from the HRIP Act apply:

- disclosure of the information is reasonably necessary to lessen or prevent a serious and imminent threat to life, health or safety of the individual or another person, public health or public safety
- disclosure of the information is reasonably necessary for the funding, management, planning or evaluation of health services and reasonable steps are taken to de-identify the information
- the disclosure of the information is reasonably necessary for the training of employees of the organisation or persons working with the organisation and reasonable steps are taken to de-identify the information
- the disclosure of the information is reasonably necessary for research, or the compilation or analysis of statistics in the public interest and reasonable steps are taken to de-identify the information
- the disclosure of the information is to provide the information to an immediate family member of the individual for compassionate reasons.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Safeguarded – An agency should only disclose sensitive personal information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership if disclosure is

necessary to prevent or lessen a serious and imminent threat to the person's life or health or that of another person.

The Department's Policy and Implementation Strategy

The Department will not disclose personal information unless it is necessary to do so to protect a person's life or health.

In accordance with its statutory function and powers, the Department hosts websites, industry events, industry newsletters, international missions/events and other co-operative advertising campaigns which disclose a limited amount of personal information to persons overseas. Additionally, international missions/events operated by the Department involve the making of a limited amount of personal information available outside the state jurisdiction. However, in each instance, the person to whom the information relates has completed an application form indicating their intention to participate in these events/programs.

Where a third party contractor undertakes a part of the service provision for the above services on behalf of the Department, the third party contractor has been contractually bound to comply with the information protection principles.

Statutory Exemptions

Statutory exemptions from the Privacy Acts apply:

- where the disclosure is necessary to investigate an offence or where there are reasonable grounds to believe an offence has been or may be committed
- where an agency is authorised or required not to comply under any Act or law
- where non compliance is "necessarily implied" or "reasonably contemplated" under any Act or law
- where the person expressly consents
- where a disclosure is required to be made to the Minister for the purpose of informing the Minister about any matter within the Minister's administration.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

IDENTIFIERS & ANONYMITY

Not identified – *an agency can only give an individual an identification number if it is reasonably necessary to carry out its functions efficiently (Health Records and Information Privacy Act only).*

The Department's Policy and Implementation Strategy

The purpose of this principle is to avoid health records being built up about an individual without their knowledge.

Employees are supplied with a personal identification number at the commencement of employment with the Department which is consistent with staffing practices in the NSW Public Service. The identifier is attached to the individual's personal file and used as an identifier for most staffing actions e.g., leave requests, payroll records. Generally, the Department has no business reason to collect health information from clients. If health information is collected from employees and clients, it will be done so with the concurrence and full understanding of the privacy implications by either the employee or the client concerned.

Anonymous – an individual is entitled to receive health services anonymously, where this is lawful and practicable (Health Records and Information Privacy Act only).

The Department's Policy and Implementation Strategy

The purpose of this principle is to provide health services where lawful and practicable.

The Department makes available a free employee assistance (counselling) service to its staff. This service is provided by an independent agency and all information is held anonymously (if requested by the individual) and "in confidence" by that agency. This Plan only applies to the practices of the Department and not the functions and processes of the Department's outsourced employee assistance provider.

The Department does not provide health services to the general community.

TRANSFERRALS and LINKAGE

Controlled – an individual's health information can only be transferred outside New South Wales if:

- 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
- the individual consents to the transfer, or
- 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
- 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
 - all of the following apply:
 - the transfer is for the benefit of the individual,
 - it is impracticable to obtain the consent of the individual to that transfer,
 - if it were practicable to obtain such consent, the individual would be likely to give it, or
- the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:
 - a serious and imminent threat to the life, health or safety of the individual or another person, or
 - a serious threat to public health or public safety, or
 - 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
 - the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

(Health Records and Information Privacy Act only).

The Department's Policy and Implementation Strategy

The purpose of this principle is to ensure that all organisations transferring/receiving health information have similar privacy standards.

The Department will comply with this principle if required to transfer health information about an individual outside NSW. Should a situation arise where the Department is required to transfer health information outside NSW, the Department will seek appropriate professional advice prior to undertaking the transfer.

Authorised – an individual's health information can only be included in a system to link health records across more than one agency if the individual expressly consents to this (Health Records and Information Privacy Act only).

The Department's Policy and Implementation Strategy

The purpose of this principle is to allow organisations to link health information and to facilitate health services.

The Department will comply with this principle if required to include an individual's health information in a system that links the individual's health records across more than one agency. Should a situation arise where the Department is required to do so, the Department will seek appropriate professional advice prior to proceeding and ensure that the individual concerned has given their consent.

Statutory Exemptions

Statutory exemptions from the HRIP Act apply:

- where an agency is authorised or required not to comply under any Act or law
- where non compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Whether any of the statutory exemptions apply will depend on the nature of the particular matter and legal advice will be obtained, if required.

Part 2 Dissemination of Privacy Policies

The Department disseminates its privacy policy through its Privacy Management Plan and a staff guidelines document called "What do I have to do?", during staff induction and staff development activities and through the distribution of privacy statements.

Privacy Management Plan and Staff Guidelines

The Privacy Management Plan and associated staff guidelines explain individual responsibilities in relation to the provisions of the Privacy Acts. These documents are made available to all staff via the Department's intranet.

Staff Induction

All new starters are made aware of the Department's obligations, policies and implementation strategies in relation to privacy management during the induction process.

Staff Awareness

Staff are provided with advice on privacy management via the Intranet and staff newsletter. Information sessions are conducted regularly for staff to ensure awareness and understanding of the obligations in collecting, storing, using and only where necessary, disclosing personal information. Staff will be informed of updates to the legislation and information sessions will be held as required.

Distribution of Privacy Statements

The Department has included a privacy statement explaining the key elements of the Privacy Acts on all its websites. The Department has included privacy statements on its information collection forms and general marketing material.

Reporting matters

The Department will issue a statement in its Annual Report concerning privacy and personal information. The Department may also include the types of personal information it holds in its FOI Act "Statement of Affairs".

Part 3 Other Relevant Matters

Privacy Codes of Practice

The Department has not developed a Privacy Code of Practice to modify the information protection principles in the Privacy Acts.

The Workforce Profile Code of Practice for the NSW Public Service covers collection of employee information which is forwarded to the Premier's Department by the Department and the CCSU as part of the Workforce Profile.

To date there have been no health privacy codes of practice made.

Public Interest Directions

Under section 41 of the *Privacy and Personal Information Protection Act 1988*, the Privacy Commissioner may make a direction to waive or modify the requirement for a public sector agency to comply with an information protection principle.

The Department has adopted the following public interest directions:

- Direction on Research (expires 31/12/2004)
- Direction on Investigations (expires 31/12/2004)
- Direction on inter-agency transfers (expires 31/12/2004).

To date there have been no health public interest directions made.

Contracts with third party contractors/consultants

The Department has contractual arrangements with a range of service providers. In some cases, these contracts are ongoing and span a number of years. Some were in existence prior to the commencement of the Privacy Acts. Existing contracts are being reviewed and updated to reflect the obligations of the Department under the Privacy Acts. New contracts will include appropriate clauses covering compliance issues.

Confidentiality and Commercial-in-Confidence

The obligations of confidentiality and commercial-in-confidence are additional to and separate from that of privacy. Nevertheless, a duty to withhold information lies at the heart of all these concepts. Confidentiality attaches to information per se, commercial-in-confidence attaches to business information and personal information to the person to whom that information relates.

Under the Department's Code of Conduct an obligation of confidentiality concerning information in general and commercial-in-confidence concerning business information exists for all employees. Information which may be confidential is also likely to have a separate and independent obligation attached to it in the form of privacy. Disclosure of information will need to be considered separately in the context of privacy and confidentiality provisions.

In respect of confidentiality provisions, the following policies will also apply:

- Code of Conduct: an ethical framework
- Protected Disclosures - Internal procedures for reporting
- Use of Communication Devices – Policy and Guidelines.

Regular review of the collection, storage and use of personal information

The Department's information handling practices relating to the collection, storage and use of personal information will be reviewed by the Department every three (3) years. Any new program initiatives will be incorporated into the review process with a view to ascertaining whether or not those programs comply with the Privacy Acts.

Regular Review of Privacy Management Plan

Once the information practices are reviewed, the Department's Privacy Management Plan will also be reviewed every three (3) years to ensure that the Plan is up to date.

Part 4 Procedures for Conducting Internal Reviews

1. Initial Discussions

The Department has a policy of providing all reasonable assistance to anyone wishing to complain about the Department's handling of their personal information (including health information). The assistance will include, in the first instance and where possible, access to and correction of personal information without the need for recourse to formal internal review procedures. Where a person, after discussion with the Privacy Contact Officer, remains concerned or dissatisfied and wishes to proceed with a formal application for internal review, the following procedures will be undertaken.

2. Application Forms for Internal Review

Applicants for internal review are assisted in the completion of their applications by the provision of an application form which ensures that all of the information required to constitute an effective application is obtained from the applicant. Specific assistance is available for people with disabilities and those who require an interpreter. A copy of the form is attached.

3. The Internal Review Process

In these procedures, the term "reviewing officer" means an officer of the Department who is qualified to deal with the subject matter of the complaint, by reason of the officer's seniority and experience, and who was not involved in the subject matter of the complaint.

On receipt of the application for review, the reviewing officer will advise the

Department's Privacy Contact Officer (i.e., Director, Business Governance) of the application and will, in conjunction with that officer, notify the Privacy Commissioner of the application and keep the Privacy Commissioner informed of the progress of the internal review. A review must be completed as soon as practicably reasonable and if not completed within 60 days from the date of receipt of the application, the applicant has a right to seek a review of the conduct by the Administrative Decisions Tribunal.

The reviewing officer will assess the application to determine whether the review will be undertaken by the Department or whether it will be undertaken by the Privacy Commissioner. Matters which will influence this assessment will include whether the applicant has made a specific request for the review to be undertaken by the Privacy Commissioner or whether review by the Department could reasonably give rise to a perception of conflict or bias. Generally, preference will be given to the review being undertaken by the Department.

Following assessment, the officer will inform the applicant in writing of the name, position and contact telephone number of the officer conducting the review or of the fact that the review has been referred to the Privacy Commissioner, if applicable. This advice will also include information about the timeframe for completing the review and the range of actions the Department may decide to take in resolving the complaint. These include:

- take no further action
- make a formal apology
- take appropriate remedial action, which may include payment of compensation
- give an undertaking that the conduct will not recur, and
- implement measures to prevent recurrence of the conduct.

The reviewing officer will take the following steps in the completion of the review:

- assist the applicant to provide all relevant information and documentation in support of the complaint, including the particulars and evidence of the alleged breach and the harm, if any, caused by the alleged breach
- interview relevant staff and examine records and obtain any other pertinent information on the circumstances of the alleged breach
- identify the nature of the breach within the terms of the Privacy Acts, that is, whether the alleged conduct breaches an information protection principle, and/or a Code of Practice
- seek advice from the NSW Office of the Privacy Commissioner, if required
- determine whether a breach has occurred and, if so, what harm or damage it has caused to the applicant
- prepare a report to the Privacy Contact Officer setting out the steps taken in the review, the conclusions reached and a recommendation for action to be taken to resolve the complaint. Letters to the applicant and to the Privacy Commissioner will accompany the report advising of:
 - the findings of the review and reasons for the findings
 - the action proposed to be taken and reasons for that action
 - the applicant's right to have the findings and the reasons for the findings reviewed by the Administrative Decisions Tribunal.

The reviewing officer will also advise the applicant in writing of the status of the review if the complaint is not resolved within 30 days of the date of the application.

4. Statistical Information on Applications and Outcomes

The Privacy Contact Officer will maintain, in secure storage, statistical information on all applications for internal review and the outcomes of those applications for inclusion in the Department's Annual Report and for the information of the NSW Privacy Commissioner.

5. External Review

People may apply to the Administrative Decisions Tribunal for a review of the action taken by the Department in conducting its review. The Tribunal may make orders requiring the Department to:

- pay to the applicant damages not exceeding \$40,000 by way of compensation for any loss or damage suffered because of the conduct (but only if the conduct occurs after 1 July 2001) and the Tribunal is satisfied that the applicant has suffered financial loss, or psychological or physical harm, because of the conduct of the public sector agency
- restrain from any conduct or action in contravention of an information protection principle or a privacy code of practice
- perform an information protection principle or a privacy code of practice;
- correct personal information that has been disclosed
- take specified steps to remedy any loss or damage suffered by the applicant;
- not disclose personal information contained in a public register; and
- follow such ancillary orders as the Tribunal thinks appropriate.

Either party may appeal the decision of the Administrative Decisions Tribunal to the Appeal Panel.

Application for Internal Review

To:
Privacy Contact Officer
Department of State and Regional Development
Level 35, Governor Macquarie Tower
1 Farrer Place
SYDNEY NSW 2000
T: (02) 9228 4622

Today's Date :.....
Your Name:.....

Residential Address:.....
Postal Address: (if different to Residential Address).....

Describe fully the circumstances and conduct which you allege constitute a breach of your privacy.

.....
.....
.....
.....

Do you know the name of the Division or section to which your complaint refers? Please specify if you can.

.....
.....

Do you have the name of any Department officers who you believe are involved?

.....

When did the conduct you are complaining about occur? Please be specific.

.....

When did you become aware of the conduct?

.....

What effect has the alleged conduct had on you?

.....
.....
.....

What effect could this conduct have on you?

.....
.....
.....

Have you suffered any financial loss as a result of the alleged conduct? If so, please specify.

.....
.....

What would you like to see the Department do about this?

.....
.....
.....

I understand that details of my application will be referred to the NSW Privacy Commissioner in accordance with S 54(1) of the PPIP Act and the Privacy Commissioner will be kept informed of the progress of the Internal Review.

.....Dated:.....
Signature of Applicant

**Notes for the person completing the application*

Your application must describe as accurately as possible the facts or circumstances which make up the complaint using, as much as possible, first hand knowledge.

Please retain a copy of your signed application.

You will receive a letter acknowledging the Department's receipt of this application within fourteen (14) days of receipt or as soon as practicable.

The complaint may be dealt with by conciliation if everyone concerned, including the Reviewing Officer is agreeable. If everyone agrees to seek to resolve the matter by conciliation, everything said in a conciliation is not admissible and otherwise confidential. If the conciliation is unsuccessful, the Reviewing Officer may have to hand the matter back to the Privacy Contact Officer for another Reviewing Officer to be appointed.

The Reviewing Officer is required to complete the review within sixty (60) days from the date you lodge your Application for review.