



**Queensland
Government**
Department of **Housing**

Information Privacy

Privacy Plan

Developed by Corporate and Executive Services
through Organisational Performance and Strategy

Approved
Linda A Apelt
Director-General
28 March 2002

PRODUCTION DETAILS

Developed by

Organisational Performance and Strategy

Authorised by

Natalie MacDonald
General Manager, Corporate and Executive Services

Edition details

Version Number: 0.5
Release Date: March 2003
Review Status: Final
Document ID: G: \ Common \ Privacy \ Plan \ Privacy Plan - Housing.doc

Amendments list

Version	Date	Additions/Amendments	Authorisation
0.1	March 2002		
0.2	March 2002	Sharon Wilson	
0.3	March 2002	Feedback from General Managers / Service Areas	
0.4	March 2002		
0.5	March 2003	Review of status of plan. Minor amendments to sections 3, 6 & 8.	

Final Version Approved By:

Name and title	Signature	Date
Name: Linda Apelt Designation: Director-General Department of Housing		/ /

Table of Contents

1. Introduction.....	3
2. What is Personal Information?	3
3. Acts Administered by Department of Housing	5
4. Personal Information held by the Department Of Housing	6
5. Types of Existing Contracts, License agreements and Out-sourcing Arrangements agreements which may contain personal information.....	10
6. Procedure to Access or Amend Personal Information.....	10
7. Complaints and Review Procedures	11
8. Implementation of Privacy Plan	13
Appendix A	16

1. Introduction

This Privacy Plan is a plan for the Department's compliance with the information privacy principles under the requirements of Information Standard 42 and its relevant Information Standard Guidelines. These eleven Information Privacy Principles (IPPs) are contained in Appendix A. The Information Standard and its relevant Guidelines requires each "Queensland Government Agency" to prepare and implement a Privacy Plan approved by the Director-General by 31 March 2002.

This plan is drafted in a way which takes account of the diverse range of functions of the Department. It provides:

- ? guidance to members of the public to assist them to understand how personal information is managed in the Department and how they can exercise their privacy rights in respect of the Department's activities;
- ? guidance to officers in the Department who deal with personal information on the requirements of the Information Standard and its guidelines; and
- ? a strategic overview for achieving full compliance with those requirements.

2. What is Personal Information?

2.1. Definitions

Information Standard 42 is concerned with "personal information". This is defined in the Information Standard as being:

Personal Information for the purposes of all Information Privacy Principles other than Information Privacy Principles 6 and 7 means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Personal Information for the purpose of Information Privacy Principles 6 and 7 is limited to information concerning an individual's "personal affairs" as the phrase "personal affairs" has been interpreted in the *Freedom of Information Act 1992*.

The information does not have to clearly identify a person. It need only provide sufficient information to lead to the identification of a person. It is not limited to confidential or sensitive personal details. It covers information held in paper records, electronic records or other media (photographs, audio tape, video tape etc.).

2.2. Exemptions

While the definition of "personal information" is very broad, there are some important exceptions to the definition. There are two sets of exemptions to Information Standard No. 42:

- ? The first set of exemptions relates to bodies that are exempt from all or part of the standard.
- ? The second set relates to personal information that is exempt from the standard.

2.2.1. Exempt Bodies

The following bodies are exempt from Information Standard No. 42:

- ? Royal commissions or commissions of inquiry;
- ? Parents and Citizens Associations as defined in Part 6 of the *Education (General Provisions) Act 1989*; and
- ? Queensland Department of Health.¹

Courts and tribunals (including the holders of office) are exempt with respect to their judicial and quasi-judicial functions only. Judicial functions include coroners exercising their powers under the *Coroners Act 1958*.

Law enforcement agencies are exempt from IPPs 2,3,9,10 and 11, for all functions except administrative functions. They are, however, bound by IPPs 1, 4, 5 and 8. As with all agencies the rights of access and correction under IPPs 6 and 7 are limited to existing rights under the *Freedom of Information Act 1992*.

2.2.2. Exempt Personal Information²

The following personal information is exempt from Information Standard No. 42:

Covert activity

- ? Personal information about an individual arising out of or in connection with a controlled operation or controlled activity within the meaning of the *Police Powers and Responsibilities Act 2000*.
- ? Personal information about an individual arising out of or in connection with a covert undertaking of an operation, investigation or function of a law enforcement agency.
- ? Personal information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth.

¹ The Queensland Department of Health is bound by Information Standard No.42A. Statutory bodies (within the meaning of the Financial Administration and Audit Act 1977) administered by the Minister for Health are, however, bound by Information Standard No. 42.

² The provisions pertaining to exempt personal information do not relieve anyone from existing requirements to obtain that personal information through either a legislative authority or under subpoena or warrant.

Witness protection

Personal information about a witness who is included in a witness protection program under the *Witness Protection Act 2000* or who is subject to other witness protection arrangements made under an Act. The Act provides for protection of their privacy.

Disciplinary actions and misconduct

- ? Personal information about an individual arising out of a complaint made under Part 7 of the *Police Service Administration Act 1990*;
- ? Personal information about an individual arising out of an investigation of misconduct or official misconduct under the *Criminal Justice Act 1989*.

Whistleblowers

Personal information about an individual that is contained in a public interest disclosure within the meaning of the *Whistleblowers Protection Act 1994*, or that has been collected in the course of an investigation arising out of a public interest disclosure. The Act protects their privacy.

Cabinet and Executive Council documents

Personal information about an individual that is contained in a document of a kind referred to in sections 36 and 37 of the *Freedom of Information Act 1992* (ie Cabinet and Executive Council documents). The Act protects their privacy.

Commissions of Inquiry

Personal information about an individual arising out of a Royal Commission or commission or inquiry.

3. Acts Administered by Department of Housing

The following Acts and Agreements are administered by the Department:

- ? *Commonwealth and State Housing Agreement (Services Personnel Act 1991)*;
- ? *State Housing Act 1945*;
- ? *State Housing (Freeholding of Land) Act 1957*;
- ? *Queensland Building Services Authority Act 1991*;
- ? *Domestic Building Contracts Act 2000*;
- ? *Subcontractors' Charges Act 1974*; and
- ? *Residential Tenancies Act 1994*.
- ? *Residential Services (Accommodation) Act 2002*.

Legislative requirements relating to personal information that will supersede the Information Privacy Principles.

- ? *Freedom of Information Act 1992*; and
- ? *Judicial Review Act 1991*.

4. Personal Information held by the Department Of Housing

The Department holds personal information in the following ways:

4.1. EMPLOYEE RECORDS

Employee records include:

- ? personnel and payroll;
- ? recruitment; and
- ? other records.

This information is held centrally in Human Resources and in each of the various Service Areas of the Department. Current and former employees and other persons (for example, spouses and next of kin who believe that the Department's personnel records may also contain personal information about them) can obtain details of specific record handling practices of particular Service Areas by contacting HR Administrators in those Service Areas.

It should not be assumed that all records described are kept in a common storage facility. Separate security arrangements will typically apply, depending on the sensitivity of the information.

The purpose of these records is to maintain employment history and payroll and administrative information relating to all permanent, contract and temporary staff members and employees of an agency.

Personnel and Payroll

These records may include any one or more of the following:

- ? records relating to attendance and overtime;
- ? leave applications and approvals;
- ? medical records;
- ? payroll and pay related records, including banking details;
- ? tax file number declaration forms;
- ? declarations of pecuniary interests;
- ? personal history files;
- ? performance appraisals, etc;
- ? records relating to personal development and training;
- ? trade, skill and aptitude test records;
- ? completed questionnaires and personnel survey forms;

- ? records relating to removals;
- ? travel documentation;
- ? records relating to personal welfare matters; and
- ? contracts and conditions of employment.

Recruitment

These records may include any one or more of the following:

- ? recruitment and selection processes;
- ? records relating to relocation of staff and removals of personal effects; and
- ? records relating to referee checks and security clearances.

Other records

These records may include any one or more of the following:

- ? records of accidents and injuries;
- ? compensation case files;
- ? rehabilitation case files;
- ? records relating to counselling and discipline matters, including disciplinary, investigation and action files, legal action files, records of criminal convictions, and any other staff and establishment records as appropriate;
- ? complaints and grievances; and
- ? recommendations for honours and awards.

Contents of employee personnel records may include: name, address, date of birth, occupation, employee identification number, gender, qualifications, equal employment opportunity group designation, next of kin, details of pay and allowances, leave details, work reports, security clearance details and employment history. It may also include physical and mental health, disabilities, racial or ethnic origin, disciplinary investigation and action, criminal convictions, adverse performance and security assessments, tax file numbers, relationship details and personal financial information.

Personal information on personnel records relates to current and former staff members and employees including contract and temporary staff.

The following departmental staff have access to most personnel records: executive and senior personnel management staff, supervisors and members of selection committees (if appropriate), and the individual to whom the record relates.

Personnel records are kept for variable periods according to the applicable provisions of the Standard Retention and Disposal schedule for staff and establishment records issued by Queensland State Archives.

Information held in personnel records may be disclosed outside the Department, as appropriate, to:

- ? Australian Taxation Office;
- ? QSuper;

- ? Office of Public Service Merit and Equity; and
- ? third parties such as banks and insurance companies (name and account numbers only).

Individuals can obtain information regarding access to their personal information by contacting the Manager, Human Resource Management (07) 322 22812 or the Department's Freedom of Information Co-ordinator (07) 322 45245.

Records relate to all current and former employees of the Department and are stored on paper and electronic media.

Location: Human Resource Management and Service Areas.

4.2. CLIENT RECORDS

The purpose of these records is to collect information for the purpose of client eligibility and assessment, tenancy management, loan and grant management, rental or subsidy calculation and property management. General content may include name, contact details and cultural background. Sensitive content may include financial position and medical information.

Client Services staff, Aboriginal and Torres Strait Islander Housing staff, Home Purchase Assistance staff, and other Housing staff within the Department may have access to this personal information.

The records are retained according to the categories set out in the standard Retention and Disposal Schedule issued by Queensland State Archives. Separate storage and security arrangements apply depending on which Service Area holds the records and the sensitivity of the information.

This information may be released to other government agencies. Where this occurs, the release of information is consistent with legislation, or, prior approval is obtained.

Individuals can obtain information regarding access to their personal information in the client service records by contacting the relevant Service Area of the Department, or the Department's Freedom of Information Co-ordinator (07) 322 45245.

Location: Service Areas.

4.3. FINANCIAL RECORDS

The purpose of these records is to process and account for expenditure and revenue. General content may include name, address and service or goods category. Sensitive content may include financial information including debts. The personal information relates to creditors and debtors, including outsourced service providers if they are identified personally.

Administration staff within the Department have access to this personal information.

The records are retained according to the categories set out in the standard Retention and Disposal Schedule issued by Queensland State Archives. Separate storage and security arrangements apply depending on which Service Area holds the records and the sensitivity of the information.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their personal information by contacting the Office of the General Manager, Housing Finance (07) 322 51777 or the Department's Freedom of Information Coordinator (07) 322 45245.

Location: Housing Finance and Service Areas.

4.4. INFORMATION SYSTEMS ACCESS RECORDS

The Department's information systems routinely stores for varying periods, information about access to departmental systems which may be personal. This includes computer access, computer activities, and computer violations.

In addition to material described above, some personal information is specifically tailored to IT system administration, including IT system security identifiers and usage tracking records.

That information is not usually disclosed to persons other than staff supervisors, system administrators and the individual officers concerned. Where information is disclosed, it is limited to provision of staff contact details for client assistance. Staff are routinely made aware of system usage rules and monitoring procedures concerning collection and use of the information.

Individuals can obtain information regarding access to their information systems access records by contacting the Manager, Information Management (07) 322 77717 or the Freedom of Information Coordinator (07) 322 45245.

Location: Information Management and Service Areas.

4.5. MINISTERIAL AND DIRECTOR-GENERAL RECORDS

Inwards correspondence, that has been addressed to the Minister / Director-General from the public or other government agencies on a wide array of matters of official business of the Minister's portfolio, may be referred to the Department for consideration and preparation of advice and responses including outward correspondence.

The Department keeps copies of the inwards and outwards documentation in electronic and paper form.

Those records may include personal information, which might arise in any subject matter related to portfolio responsibilities. Examples are: names, addresses, personal opinions about public administration matters, occupational and organisational information about persons, complaints and grievances, and any other matter that the

correspondent wishes to convey to the Minister / Director-General about themselves or personally identifiable third parties in government or amongst the public.

The departmental staff who have access to the ministerial correspondence records are executive and senior officers, administrative staff who process the correspondence and departmental officers on a “need to know basis”. The information is not usually disclosed to other persons or organisations.

The records under the control of the Department containing the personal information are retained for periods provided under the standard Retention and Disposal Schedule authorised by State Archives.

Individuals can obtain information regarding access to their personal information in the ministerial correspondence records by contacting the Executive Services Unit of the Department, the relevant Service Area of the Department, or the Department’s Freedom of Information Co-ordinator (07) 322 45245.

Location: Executive Services and Service Areas.

5. Types of Existing Contracts, License agreements and Out-sourcing Arrangements agreements which may contain personal information

The Department of Housing enters into contractual arrangements with a variety of external parties for the supply of goods and services to the Department. The duration of these agreements varies widely with some extending over several years. These contractual arrangements have been in existence prior to the Department’s requirement to comply with the privacy principles in contractual arrangements.

If existing contracts are renewed, they will be reviewed and amended to comply with the privacy principles. Any new contracts will comply with the privacy principles.

6. Procedure to Access or Amend Personal Information

Under the privacy scheme, there are controls on how *personal information* is managed. The rights of access and amendment are dealt with in Information Privacy Principles (IPPs) 6 and 7. Those rights are confined to the person to whom the personal information directly and personally relates.

IPP 6 provides that a person is entitled to access any record that contains their *personal information* except where access is restricted by any law.

IPP 7 provides that a person is entitled to seek an amendment of any record that contains their *personal information* which is misleading, irrelevant, not up-to-date or incomplete.

However, Information Standard 42, in which Information Privacy Principles 6 and 7 appear, qualifies those access and amendment rights by saying that they are limited to

existing rights under the *Freedom of Information Act 1992*. This means that *personal information* for the purpose of IPPs 6 and 7 is limited to information concerning an individual's *personal affairs* in the way that phrase has been interpreted in the *FOI Act*.

In summary, if a request is made to access or amend personal information records in the Department of Housing;

- ? **the IPPs limit the access and amendment rights and processes to those provided in the *FOI Act*; and**
- ? **any application for documents or application for correction or amendment will therefore be processed under the *FOI Act* provisions.**

Persons wanting to make an FOI access or amendment application can obtain help from the Department's Internet website at:

http://www.housing.qld.gov.au/publications/statement_of_affairs_2002/foi_forms.htm

Assistance is also available from the Department's Freedom of Information Coordinator. The telephone contact number is (07) 322 45245.

7. Complaints and Review Procedures

If an individual believes that their personal information has not been dealt with in accordance with an Information Privacy Principle (IPP), they may make a complaint to the Department. A complaint must be made in writing within six months from the date when the breach was suspected to have occurred.

Written complaints should be sent to:

FOI Coordinator
Department of Housing
GPO BOX 2457
BRISBANE QLD 4001

Or by facsimile: (07) 322 46938

The FOI Coordinator can provide more information about complaint handling procedures and can be contacted on (07) 322 45245.

Complaints will be acknowledged in writing within 14 days from the date on which the written complaint was received. The Department will aim to process each complaint within 60 days from the date on which it is received.

The complainant will be advised in writing of the Department's complaint investigation decision, including any remedies that are considered appropriate to resolve the complaint.

If a complainant does not agree with the Department's decision, they may request an internal review. Applications for internal review must be made in writing within 28 days

of the complainant receiving the initial complaint decision notice. The postal address for internal review applications is:

Internal Review Officer (Privacy)
Legal and Contractual
Department of Housing
GPO BOX 2457
BRISBANE QLD 4001

The internal review will be carried out by an officer who is no less senior than the initial decision-maker and who has not previously been involved in the matter. The internal review will be completed within 45 days of receipt of the application for internal review.

The Internal Review Officer will provide a decision in writing to the individual who requested the further review.

8. Implementation of Privacy Plan

The Department of Housing will fully implement the privacy plan by September 2003. The steps to implement the privacy plan are set out below. In addition, informing staff of their privacy responsibilities will play a critical role in successfully complying with the requirements of IS 42 and related guidelines. To ensure a general awareness of the issues and the principles involved, mechanisms have been identified which will provide ready access by staff to information regarding the Plan and the distribution of the Information Privacy Principles which form the core of Information Standard 42.

Objective	Implementation
Increase awareness of privacy responsibilities	Inform staff of the content and implementation steps of the Privacy Plan. <i>Completed</i>
	Provide the website address of the Privacy Plan to executives, managers and work unit supervisors. <i>Completed</i>
	Provide information on privacy responsibilities to senior management and line management. <i>Ongoing</i>
Provide training on privacy Issues	Advise the Housing Board of Management of privacy issues. <i>Ongoing</i>
	Incorporate privacy issues into line manager/supervisor training. <i>Completed</i>
	Incorporate privacy issues into staff training programs. <i>In progress</i>
	Incorporate privacy issues in new staff induction and orientation programs. <i>Completed</i>
Review relevant policies/guidelines	Review relevant policies and guidelines to integrate privacy issues where appropriate. <i>In progress</i>

Objective	Implementation
	Review and upgrade grievance documentation to include privacy complaints. <i>In progress</i>
	Review and upgrade procedures for dealing with subpoenas, law enforcement officers, and external requests for access. <i>In progress</i>
Review legislation	Identify any statutory requirements that will supersede the requirements of the IPPs. <i>Completed</i>
Develop complaint handling procedures	Develop guidelines and procedures on complaint handling and resolution. <i>Completed</i>
Review contracts	Review any agency contracts, license agreements for compliance with the IPPs. <i>Completed</i>
Review all notices, applications, forms, questionnaires etc.	Review all notices, applications, forms, questionnaires etc. to ensure compliance. Modify where necessary. Where stocks of forms exist, attach information flyers as an interim measure to ensure compliance with IPP 2. <i>In progress</i>
Ensure all sectors of public can be notified of the Privacy Scheme	Develop and disseminate multi-lingual privacy statements for non-English speaking clients. <i>In progress</i>
Develop privacy policies/guidelines	Develop an entry in the Statement of Client Service regarding clients' rights and responsibilities with regard to privacy. <i>Privacy has been developed as a sub-set of the Statement of Client Service.</i>
	Develop guidelines to be given to contractors regarding privacy responsibilities. Review and upgrade terms of contracts to progressively accommodate privacy compliance. When current licenses or contracts cease, new ones must comply with IS 42 and guidelines. <i>In progress</i>

Objective	Implementation
	<p>Ensure records management policies comply with IS 42 and guidelines. <i>Ongoing</i></p>
	<p>Develop guidelines for the storage and security of personal information to comply with IS 42 and IS 18 (Information Security). <i>In progress</i></p>
	<p>Develop guidelines for client service areas where personal information is collected. <i>In progress</i></p>
	<p>Develop guidelines for staff with special responsibilities for personal information (eg: human resources, counselling, health and safety, employment and service equity). <i>In progress</i></p>
	<p>Develop guidelines for all staff regarding privacy responsibilities. <i>In progress</i></p>
<p>Conduct annual review</p>	<p>Conduct annual review and update of Privacy Plan. <i>Ongoing</i></p>
<p>Monitor privacy awareness</p>	<p>Conduct periodic surveys to monitor changes in privacy practice and awareness. <i>Ongoing</i></p>
<p>Monitor changes to Privacy and Security Statement</p>	<p>A Security Statement will be provided when payments are made to the Department through the Internet.</p>
<p>Monitor changes to Internet site development</p>	<p>Changes will be made to the Privacy and Security Statement if there is any change to the usage of 'cookies'.</p>

Appendix A

10.A. Summary of Information Privacy Principles

Policy Statement

Personal information held by Queensland agencies must be responsibly and transparently collected and managed (including any transfer or sale of personal information held by agencies to other agencies, other levels of Government or the private sector) in accordance with the requirements of the Information Privacy Principles.

Policy Principles

Agencies must comply with eleven IPPs, which govern how personal information is collected, stored, used and disclosed.

The IPPs deal with the following:

- ? Principle 1: Manner and purpose of collection of personal information;
- ? Principle 2: Solicitation of personal information from individual concerned;
- ? Principle 3: Solicitation of personal information generally;
- ? Principle 4: Storage and security of personal information;
- ? Principle 5: Information relating to records kept by record-keeper;
- ? Principle 6: Access to records containing personal information;
- ? Principle 7: Alteration of records containing personal information;
- ? Principle 8: Record-keeper to check accuracy, etc., of personal information before use;
- ? Principle 9: Personal information to be used only for relevant purposes;
- ? Principle 10: Limits on use of personal information;
- ? Principle 11: Limits on disclosure of personal information.

Collection of Personal Information (IPPs 1-3)

Information Privacy Principle 1

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
 - (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
 - (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Information Privacy Principle 2

Where:-

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:-

- ? the purpose for which the information is being collected;
- ? if the collection of the information is authorised or required by or under law, the fact that the collection of the information is so authorised or required; and
- ? any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Information Privacy Principle 3

Where:-

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:-

- ? the information collected is relevant to that purpose and is up to date and complete; and
- ? the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Storage and Security (IPPs 4-5)

Information Privacy Principle 4

A record-keeper who has possession or control of a record that contains personal information shall ensure:

- (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
- (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Information Privacy Principle 5

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:
 - (a) whether the record-keeper has possession or control of any records that contain personal information; and
 - (b) if the record-keeper has possession or control of a record that contains such information:
 - ? the nature of that information;
 - ? the main purposes for which that information is used; and
 - ? the steps that the person should take if the person wishes to obtain access to the record.
2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the State that provides for access by persons to documents.
3. A record-keeper shall maintain a record in the form of a privacy plan setting out:
 - ? the nature of the records of personal information kept by or on behalf of the record-keeper;
 - ? the purpose for which each type of record is kept;
 - ? the classes or types of individuals about whom records are kept;
 - ? the period for which each type of record is kept;

- ? the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
 - ? the steps that should be taken by persons wishing to obtain access to that information.
4. A record-keeper shall make the record maintained under clause 3 of this Principle available for inspection by members of the public.

 **Access and Alteration (IPPs 6-7)**

Information Privacy Principle 6⁴

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the State that provides for access by persons to documents.

Information Privacy Principle 7⁵

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:
- ? is accurate; and
 - ? is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.
2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the State that provides a right to require the correction or amendment of documents.

⁴ This principle deals with right of access. One of the reasons for enactment of the *Freedom of Information Act 1992* was because "Parliament recognises that in a free and democratic society ... members of the community should have access to information held by government in relation to their personal affairs and should be given ways to ensure that information of that kind is accurate, complete, up-to-date and not misleading" [Section 5(1)]. Part 3 of that Act allows for access to documents. Right of access under IPP 6 is limited to existing rights under the *Freedom of Information Act 1992*.

⁵ This principle deals with the right of amendment or correction. Part 4 of the *Freedom of Information Act 1992* deals with amendment or correction. Right of amendment or correction under IPP 7 is limited to existing rights under the *Freedom of Information Act 1992*.

3. Where:-

- (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
- (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provision of a law of the State;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Accuracy (IPP 8)

Information Privacy Principle 8

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Use and Disclosure (IPPs 9-11)

Information Privacy Principle 9

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Information Privacy Principle 10

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
 - (a) the individual concerned has consented to use of the information for that other purpose;
 - (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
 - (c) use of the information for that other purpose is required or authorised by or under law;

- (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
 - (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.
2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Information Privacy Principle 11

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
- (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
 - (b) the individual concerned has consented to the disclosure;
 - (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
 - (d) the disclosure is required or authorised by or under law; or
 - (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.
3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.