



Information Standard No 42

Information Privacy

DOCUMENT CONTROL

Document Details

Document Reference/Name: IS42_V1.00.01

Version Number: V1.00.01

Documentation Status: Working Draft RFC IS Archived

GIA Domain: Information Management

Next Scheduled Review Date September 2002

Version History

Version Number	Date	Reason/Comments
V1.00.00	September 2001	Endorsed
V1.00.01	September 2002	Minor Amendments to replace reference to <i>Libraries and Archives Act 1988</i> with <i>Public Records Act 2002</i>

Contents

- 1. Overview/Purpose 2**
- 1.1. Scope..... 2**
- 1.2 Exemptions 3**
 - 1.2.1 Exempt Bodies..... 3
 - 1.2.2 Exempt Personal Information..... 4
- 1.3 Codes of Practice 5**
- 2. Policy Statement..... 7**
- 3. Policy Principles 7**
- 3.1. Mandatory Requirements..... 7**
 - 3.1.1 Information Privacy Principle 1 8
 - 3.1.2 Information Privacy Principle 2 8
 - 3.1.3 Information Privacy Principle 3 8
 - 3.1.4 Information Privacy Principle 4 9
 - 3.1.5 Information Privacy Principle 5 9
 - 3.1.6 Information Privacy Principle 6² 10
 - 3.1.7 Information Privacy Principle 7³ 10
 - 3.1.8 Information Privacy Principle 8 11
 - 3.1.9 Information Privacy Principle 9 11
 - 3.1.10 Information Privacy Principle 10 11
 - 3.1.11 Information Privacy Principle 11 11
- 4. Authority 12**
- 5. Guidelines..... 12**
- 6. References/Supporting Documentation 12**
- 7. Definition of Terms 13**
- ATTACHMENT A - Implementation Schedule 15**

1. Overview/Purpose

The purpose of this information standard and guidelines is to establish a framework for the responsible collection and handling of personal information in the Queensland Government public sector.

In December 2000 Cabinet decided that:

- A privacy scheme be introduced to give effect over time to the Commonwealth Government public sector Information Privacy Principles (IPPs) contained in the Commonwealth *Privacy Act 1988* in the Queensland public sector.
- The privacy scheme should be implemented by administrative means, including an Information Standard and supporting privacy guidelines.
- The Information Standard and guidelines cover the transfer and sale of personal information held by agencies to:
 - other agencies,
 - other levels of Government; and
 - the private sector.
- Agencies will develop privacy plans to give effect to the agreed IPPs.
- The Department of Justice and Attorney-General (JAG) have lead agency responsibility for the privacy framework, including the provision of ongoing guidance and support for agencies.
- Responsibility for resolution of any complaints of breaches of privacy rests with chief executives of public sector entities in keeping with agency level responsibilities for addressing complaints associated with breaches of a code of conduct.

It was also decided that a review should be conducted within two years of implementation of the privacy scheme, at which time the need for specific privacy legislation would be considered.

1.1. Scope

Information standards are issued under the authority of ss. 22(2) and 56(1) of the *Financial Management Standard 1997* and apply to:

- all accountable officers; and
- statutory bodies

as defined under the *Financial Administration and Audit Act 1977*.

This information standard and guidelines will also apply to any statutory Government Owned Corporation (GOC) and its subsidiaries where the shareholding minister has given notification pursuant to s. 123 of the *Government Owned Corporations Act 1993*.

Information Standard No. 42 requires personal information to be managed in accordance with a set of IPPs adapted from the Commonwealth Government public sector IPPs contained in the *Privacy Act 1988 (Cth)*. It should be noted that the requirement for agencies to comply with the Information Standard and guidelines is administratively based. This means that:

- where conflicting requirements exist any legislative requirements will supercede compliance with the Information Standard;
- compliance is subject to any existing outsourcing arrangements, contracts and licenses. Any future outsourcing arrangement, contracts and licenses will be expected to comply with Information Standard 42. Where any existing outsourcing arrangements, contracts or licenses contemplated a future privacy regime (for example, where privacy clauses were written into a contract or license in anticipation of a future privacy regime) it may be possible to re-negotiate these terms.

1.2 Exemptions

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

1.2.1 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;
- Queensland Department of Health ¹.

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.

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.²

1.2.2 Exempt Personal Information³

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;

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;

Disciplinary actions and misconduct

- Personal information about an individual arising out of a complaint made under Part 7 of the *Police Service Administration 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;

² This means that law enforcement agencies are 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*

³ 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

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).

Commissions of Inquiry

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

1.3 Codes of Practice

Information Standard No. 42 permits codes of practice.

A code of practice may modify the application of any one or more of the IPPs to an agency, but may not modify IPPs themselves.

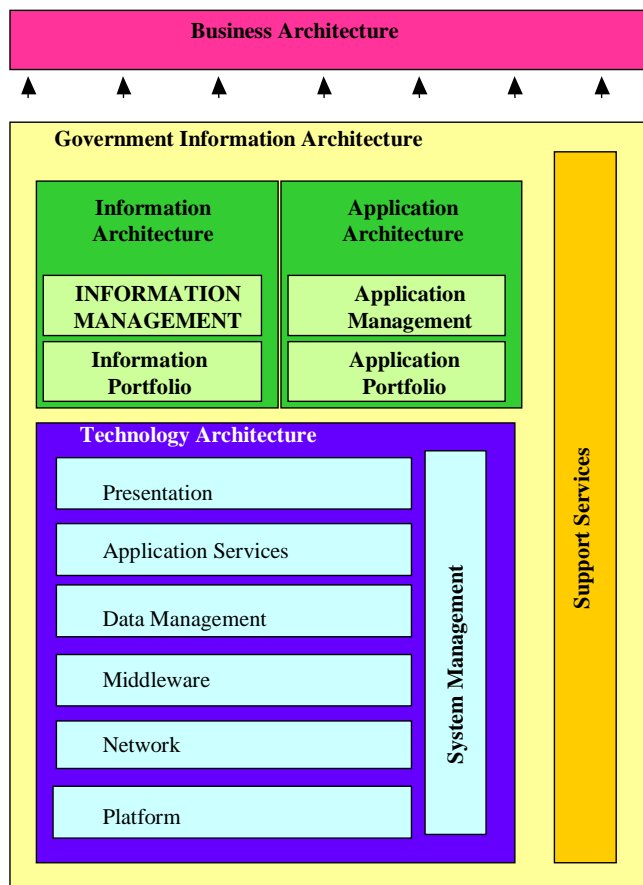
Codes can apply to any one or more of the following:

- any specified class of personal information,
- any specified agency or class of agency,
- any specified activity or specified class of activity.

Codes of Practice are to be developed by the responsible agency, approved by the Department of Justice and Attorney-General (after consultation with the Department of Innovation and Information Economy, Sport and Recreation Queensland, if appropriate) and then issued by the responsible agency. Once issued, codes are to be published together with Information Standard No. 42.

This Information Standard fits within the Information Management Domain of the GIA Reference Framework (illustrated below).

GIA Reference Framework



2. 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.

3. 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.

3.1. Mandatory Requirements

It is mandatory that departments and agencies:

- nominate a privacy contact officer who will be the first point of contact for privacy issues within their own agencies. The privacy contact officer may also, at the discretion of the agency CEO, be the first point of contact for any privacy complaints made to the agency;
- develop privacy plans to give effect to the information privacy principles (Sections 3.1.1 through 3.1.11 of this Standard), for approval by the CEO of each agency;
- publish privacy plans on their websites;
- implement the privacy plans according to a schedule developed in the privacy plan, subject to any existing contractual obligations, licenses, or other outsourcing arrangements;
- review and update privacy plans annually;

- develop and place on their website a privacy and security statement;
- be responsible for accessing and correcting records; and
- be responsible for complaint resolution mechanism.

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.1.6 *Information Privacy Principle 6*²

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 authorized 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.

3.1.7 *Information Privacy Principle 7*³

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.
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

² 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*.

³ 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*.

- (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.

3.1.8 *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.

3.1.9 *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.

3.1.10 *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.

3.1.11 *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.

4. Authority

On 11 December 2000 Queensland Cabinet approved that a privacy scheme be introduced to give effect over time to the Commonwealth IPPs in the Queensland public sector. Cabinet also decided that the scheme was to be implemented by administrative means, including an Information Standard and supporting privacy guidelines (refer to Section 1). This Information Standard was approved by Cabinet in September 2001.

5. Guidelines

Refer to the Information Privacy Guidelines.

6. References/Supporting Documentation

Commonwealth Attorney-General's Department (<http://www.law.gov.au/privacy>) [2001, February 7]

Federal privacy handbook: a guide to federal privacy law and practice (North Ryde, NSW: CCH, 1992)

Office of the Federal Privacy Commissioner (<http://www.privacy.gov.au>) [2001, February 7]

Privacy NSW: Office of the New South Wales Privacy Commissioner (<http://www.lawlink.nsw.gov.au/pc.nsf/pages/index>) [2001, February 7]

7. Definition of Terms

Collector

- Where an agency collects personal information the agency is regarded as the collector in relation to that information
- Where personal information is collected by an individual in the course of their employment by, or in the service of, an agency then the agency is regarded as the collector in relation to that information

Consent means express consent or implied consent.

Generally available publication means a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public.

Individual means a natural person.

Individual concerned, in relation to personal information or a record of personal information, means the individual to whom the information relates.

Information Privacy Principle means any of the Information Privacy Principles set out in Section 3 of this Information Standard.

Law enforcement agency for the purposes of this Information Standard means the Queensland Police Service, the Criminal Justice Commission, and the Queensland Crime Commission.

Lead agency for the purposes of this Information Standard means the Department of Justice and Attorney-General.

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*.

Record means:

- a document; or
- a database (however kept); or
- a photograph or other pictorial representation of a person;

but does not include:

- a generally available publication; or
- anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or
- public records as defined by subsection 2(2) of the *Public Records Act 2002* that are in the open access period as defined in the regulation to that Act; or
- letters or other articles in the course of transmission by post.

Solicit, in relation to personal information, means request a person to provide that information, or a kind of information in which that information is included.

Use, in relation to personal information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication.

ATTACHMENT A - Implementation Schedule

Agency privacy plan with implementation schedule completed and approved by agency CEO	[Date to be 6 months from date of Cabinet endorsement of Information Standard and guidelines]
<ul style="list-style-type: none"> • Copy of agency privacy plan published on agency website • Privacy and security statement placed on agency website 	[Date to be 15 days after date privacy plan completed and approved]
Update privacy plan as appropriate	Annually