# Table of Contents

1. INFORMATION PRIVACY ................................................. 4

2. ACTS ADMINISTERED BY QUT ..................................... 4

3. PERSONAL INFORMATION HELD BY QUT ......................... 5
   3.1 Public registers .................................................. 5
   3.2 Categories of personal information at QUT ................ 5
      A. Student records .............................................. 5
      B. Staff records ............................................... 6
      C. Human research participants ............................ 8
      D. Links to the community .................................. 9
      E. Business and financial information .................. 9
      F. Information technology records ....................... 10

4. EXISTING CONTRACTS, LICENCES AND OUTSOURCING ARRANGEMENTS ........................................................................ 11

5. RESPONSIBILITY FOR PRIVACY AT QUT ...................... 11

6. IMPLEMENTATION ...................................................... 12

7. ACCESS AND AMENDMENT PROCEDURES (IPPS 6 AND 7) ................................................................. 12
   7.1 Access arrangements at QUT ................................. 12
   7.2 Requests for amendment of information ................. 13
   7.3 Further information ............................................. 13

8. PRIVACY COMPLAINTS .................................................. 13

APPENDIX 1 – INFORMATION PRIVACY PRINCIPLES (FROM INFORMATION STANDARD 42) ............................................................ 15
Introduction

Queensland University of Technology's functions necessitate the collection and use of personal information about our students, staff and other clients. QUT recognises that, in collecting, storing and using this information, we have obligations for the protection of personal privacy.

QUT’s commitment to protecting privacy is part of a broader framework of privacy compliance requirements applying to Queensland government departments and agencies, including statutory authorities such as QUT. The privacy regime is found in Information Standard No 42 - Information Privacy (IS42) and supporting guidelines. Implementation of this standard by QUT is mandatory, as the standard has been issued under the Financial Administration and Audit Act 1977.

IS42 states that personal information held by Queensland agencies must be responsibly and transparently collected and managed in accordance with 11 Information Privacy Principles (IPPs) adapted from the Commonwealth Privacy Act 1988. The IPPs govern how personal information is collected, stored, used and disclosed.

IS42 requires that agencies develop a privacy plan to give effect to the information privacy principles. The plan is designed to assist members of the public and the University community to understand how personal information is managed in QUT and how they can exercise their privacy rights in respect of the University’s activities.

Accordingly, this plan explains QUT’s privacy framework, including the type of personal information which is collected about individuals and QUT’s practices for its use and management. The plan also describes our implementation strategy and complaint mechanisms.

The information in the plan is correct as at June 2004.

Professor O P Coade
Vice-Chancellor
1. Information Privacy

The Information Privacy Principles (IPPs) which are articulated in IS42 apply to “personal information”. “Personal information” has a very broad meaning, and has been defined in IS42 (for the purposes of all IPPs except IPP 6 and IPP 7) as “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”. IS42 excludes certain types of information from the application of the IPPs, but these exclusions will only be relevant to the University in limited circumstances.

The Information Privacy Principles fall into four broad categories, governing:

- Our activities for collection of personal information (IPPs 1-3);
- How we manage and secure our personal information records internally (IPPs 4 and 8);
- How individuals may obtain access to personal information and pursue rights to amend it (IPPs 5-7);
- Our practices for use and disclosure of personal information (IPPs 9-11).

Full details of the IPPs can be found in Appendix 1 or at www.iie.qld.gov.au/comminfo/guidelines.html.

2. Acts administered by QUT

Whilst QUT must comply with the provisions of a number of Acts of Parliament, our principal responsibility is for the administration of the Queensland University of Technology Act 1998 (the QUT Act). This Act outlines our governance arrangements and our general powers and functions as a University.

Because the privacy regime is administratively based, IS42 is overridden by any legislative requirements relating to collection, access and amendment, use or disclosure of personal information where those requirements are in conflict with the Information Privacy Principles.

QUT, together with other statutory authorities, is subject to the requirements of a number of Acts which contain provisions superseding the IPPs. For example, requirements for disclosure of information in the Freedom of Information Act 1992 (Qld) override the IPPs, as do relevant provisions relating to public records that are in the open access period under the Public Records Act 2002 (Qld). The University is also required to provide, either routinely or upon formal request, personal information to Commonwealth Government departments or agencies pursuant to various Commonwealth Acts, such as income tax legislation, the Higher Education Support Act 2003 and the Education Services for Overseas Students Act 2000.
3. Personal information held by QUT

3.1 Public registers

A public register is a register of personal information that is required by law to be made publicly available or open to public inspection (whether or not on payment of a fee). QUT is not required to maintain any public register. However, given that one of our primary functions is to confer higher education degrees and awards, QUT does maintain a register of its graduates. Information concerning a person’s status as a graduate of the University is available to any member of the public upon formal request.

3.2 Categories of personal information at QUT

Other personal information collected and held by QUT falls into the six broad categories listed below. The records listed are kept for variable periods according to the applicable provisions of the *QUT General Disposal Schedule*, which is approved by Queensland State Archives.

The steps that can be taken by persons wishing to obtain access to information concerning them are outlined in section 7 of this privacy plan.

A. Student records

One of QUT’s primary functions is the education of its students. Consequently, the University collects and holds personal information about students for the purpose of administering enrolment and education of students, and in facilitating and providing access to academic and support services, including library and information technology services. Student information held by the University for current and, where required, for former students, can be summarised as follows:

- Personal details, including date of birth, postal and permanent home address, emergency contact information;
- Statistical information, including equity group membership and educational background;
- Admission, enrolment, course progress and attendance records;
- Records relating to student examinations and assessment, including student grades;
- Records relating to industrial experience, practicums or clinical placements undertaken by students;
- Details relating to payment of fees and charges and/or HECS contribution (which may include tax file number information);
- Records relating to student welfare matters, including use of student support services in areas such as health, disability, learning assistance and personal and careers counselling; and student complaints and grievances;
- Records relating to applications for and award of prizes, scholarships and grants and other forms of student assistance;
- Library borrowing records;
- Graduation records, including information on graduate employment outcomes;
- Immunisation status and first aid qualifications (for students in specified courses only);
• Records of student members on University and faculty committees.

Much student personal information, particularly as it relates to enrolment, course progression, student grades and fee information, is held in the Student Business Services Department, in the computerised student information system or in other physical and electronic records of that department.

However, some student records are held by other organisational units. The faculty which administers the course in which the student is enrolled will, for instance, hold records relating to course progress, prizes and scholarships, industrial experience and clinical placements, and immunisation status. Records relating to student welfare matters or student usage of services will be held by the organisational unit which provides the service (for example, Health Services, Teaching and Learning Support Services, Library, etc).

Staff of the University have access to these records only as required to carry out their duties. Access to student records of the Student Business Services Department is routinely granted to administrative and technical staff of that department and to administrative and senior academic staff in faculties and schools, and to staff in other organisational units providing student services.

Access to student records held in other parts of the University is necessarily more limited, both by functional requirements, and occasionally, by the need to treat these other records with greater confidentiality. In general, access to these records will be limited to the administrative and executive staff of the organisational unit concerned, though the records may be made available to other senior staff if necessary.

Where necessary, student personal information will be disclosed outside the University to:

• Australian Taxation Office;
• Queensland Tertiary Admissions Centre (and other tertiary admission organisations in other states);
• Department of Education, Science and Training;
• QUT Student Guild (in relation to Guild membership, and for Guild election purposes);
• External organisations in which students undertake industrial or clinical placements or professional experience;
• Consultant student service providers (mailing houses, etc);
• Student's financial institution (where required for payment of student fees and charges);
• Law enforcement, intelligence gathering or revenue protection agencies (where 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.

B. Staff records

Personal information concerning QUT staff is used to administer human resource management functions, to maintain staff electoral rolls for election of members to various University committees, and for other elections in which staff participate, and to facilitate access to library, information technology and other services which are available to staff, such as parking. Records relating to current and former staff may include the following:
• Recruitment records, including position applications, records of selection processes, records of any employment checks, evidence of previous qualifications and information relating to relocation and removal of appointees;
• Appointment records (including records of casual staff) and records of leave and attendance;
• Personal details, such as date of birth, home address and phone number, emergency contact details;
• Salary and payroll information, including banking details and tax file number information, and salary packaging benefits;
• Superannuation records;
• Personal development and training records;
• Performance planning and management records and evaluations of teaching performance (academic staff);
• Records of staff health and safety requirements (including, where required, vaccination status and details of first aid certificate holders) and of accidents and injuries, including compensation and rehabilitation arrangements;
• Records relating to staff welfare matters, such as staff study assistance;
• Records relating to grievances and complaints, and industrial issues affecting individual staff;
• Staff equity data;
• Personal promotion information (academic staff);
• Library borrowing records, and other records where staff use QUT services such as the Health Service;
• Information concerning visiting researchers or adjunct staff, and other individuals providing services to the University in a voluntary capacity;
• Information concerning grants, awards, honours and recognition schemes for staff;
• Information concerning staff research output and publications, and staff participation in external and commercial consultancies;
• Information concerning staff travel;
• Records of staff membership on University and faculty committees.

Much staff personal information, particularly as it relates to recruitment, appointment, attendance and other personnel or industrial or workers’ compensation processes, is held in QUT’s computerised staff information system, or in the physical records of the Human Resources Department. Access to information is restricted to staff of the Human Resources Department, and to other staff only as required to carry out their duties.

Some functions for the management of staff are the responsibility of the organisational unit in which the staff member is employed, and consequently, some records may be held in faculties or schools or in the relevant department within a Division (for instance, timesheets and attendance records).

In addition, information concerning research grants and research output are the responsibility of the Division of Research and Commercialisation, and teaching evaluation information will be held within the Division of Technology, Information and Learning Support.

Access to staff records held in other parts of the University is necessarily more limited, both by functional requirements, and occasionally, by the need to treat these other records with greater confidentiality. In general, access to these records will be limited to the administrative and executive staff of the organisational unit concerned, though the records may be made available to other senior staff if necessary.
Disclosure outside the University occurs only in limited circumstances to:

- Australian Taxation Office;
- Superannuation providers;
- WorkCover and rehabilitation providers;
- Staff member’s financial institution (payment information only);
- Health insurers (contribution payment information only).

C. Human research participants

Research involving humans is conducted in a large number of disciplines in most faculties of the University. Consequently, QUT researchers (including students undertaking research training) may collect or use research data in the form of personal information about identified individuals, to advance knowledge or test theories or hypotheses in an area of scholarship.

The type of personal information which may be collected, used and stored for research purposes is varied, but is naturally dependent on the subject of the research project. QUT conducts behavioural or social sciences research in fields such as education, psychology, public health and management. In addition, QUT conducts research in health and biomedical fields. Personal information will therefore include medical or health information about research participants (including biological or genetic information). The research data of a personal nature may be collected directly from participants (for example, by observation or by completing questionnaires, other surveys or interviews) or it may be obtained from another organisation. Where a researcher proposes to use personal information collected for another purpose, an initial approach to the potential participant is generally made by the custodian of the information.

The use of personal information generated from research on human participants may take various forms. For instance, the identity of the individual may remain linked to the data at all times. Alternatively, the identifying information may be replaced by the use of a code, where that code is available to re-identify the individual concerned. Where any identifying information has been completely removed from the research data, then no personal information is involved.

Use of personal information about human research participants is tied to processes for obtaining ethical approval for the conduct of the research. Prior to obtaining ethical approval, a researcher must specify the particular personal information collected, describe how it will be used in the research project and explain how these processes will be explained to potential participants. To the extent possible, researchers are encouraged to obtain the informed consent of research participants prior to the collection or use of the research data.

QUT’s Code of Conduct for Research (MOPP D/2.6) specifies that research data is held in the faculty, school or centre in which the research was conducted. The responsibility for maintenance and retention of the data will lie with the head of the relevant school, centre or research concentration in which the research was generated. Individual researchers may hold copies of the data. Research data is held for a minimum of five years following publication. For clinical research, a period of 15 years is generally recommended.

The research data may be accessed by members of the research team, members of the research funding body (if appropriate), academic and administrative staff who
require access to assist the researcher(s) in a supporting role, and by senior staff of the University in limited circumstances.

Research data involving personal information is not normally disclosed outside the University. If data is to be disclosed to a third party, prior consent for the disclosure will be obtained at the time of collection or when consent for participation in the research project is obtained.

D. Links to the community

One goal of QUT is to enhance links to the community we serve and to the professions for which we train our graduates. Consequently, QUT maintains personal information relating to members of the community and the professions who are supporters of QUT teaching and research programs or who use our community services and facilities. Records containing personal information include:

- Database of QUT alumni, former staff, donors and other prospective donors;
- Mailing lists for members of the professions and users of other University facilities such as QUT Cultural Precinct;
- Records of members of the community and the professions who serve on University and faculty committees;
- Records of continuing professional education participants;
- Patient records for clients of University clinics.

Records relating to QUT’s links to the community will be held in the organisational unit which has responsibility for maintaining and enhancing these links. For instance, records relating to alumni, donors and continuing professional education services are the responsibility of the Division of International and Development, and consequently, records are maintained there, both in physical and electronic formats. The relevant faculty or school will maintain clinic records and records of community members involved in the teaching and research programs of the faculty or school.

Access to records is granted to staff only as required to carry out their duties. In general, access will be limited to administrative and/or academic staff who are directly responsible for the administration of the function involved, and other senior staff in limited circumstances where required. However, as University clinics operate in conjunction with the teaching programs of the relevant faculty or school, access to patient records will also be granted to students under the supervision of qualified teaching staff and only for teaching and learning purposes.

The records are not generally disclosed outside the University, though continuing professional education records may be disclosed to the Queensland Tertiary Admissions Centre where a participant seeks admission into a QUT award course.

E. Business and financial information

Personal information such as name, address for payment, and bank account details, is collected from vendors, suppliers, customers and contractors to facilitate electronic ordering or payment of accounts as part of normal business processes. Information concerning vendors, customers, suppliers and contractors will frequently relate to business entities rather than individuals, but personal information in the form of company representatives or contacts may be collected.
Financial records containing personal information may include:

- Records of accounts payable, including creditors and debtors of the University;
- Customer records of business operations, such as the QUT Bookshop and the Gardens Theatre;
- Job tracking systems for service providers within the University, such as the Publications and Printing Unit;
- Lists of contractors providing professional services in the building and project management area;
- Tender documents.

Most of the records listed above are maintained in financial management information systems maintained by Financial Services. Other areas such as Commercial Services, Facilities Management or the Bookshop will maintain business records relevant to their operations as appropriate.

Access to records is granted to staff only as required to carry out their duties. In general, access will be limited to administrative staff who are directly responsible for the function involved, and other senior staff in limited circumstances. External auditors from the Queensland Audit Office will also have access to these records upon request.

These records are not routinely disclosed outside the University.

F. Information technology records

QUT's information technology management systems and networks routinely carry, enable processing of, and store for varying periods, much of the core business and the support services of the University.

Information technology records encompass both internal electronic transactions and external transactions, including telephone, email and internet activity. The great bulk of the personal information records within the QUT network environment are described in section A-E above. However, in addition, there are some personal information records specifically tailored to IT systems administration, such as authentication and identification card systems, and usage tracking systems.

These records are not routinely disclosed outside the University, though in limited circumstances, information about staff will be supplied to outside organisations such as the Queensland Tertiary Admissions Centre to facilitate access by those staff to external IT systems if required for business processes.

The records are generally accessible only to IT support staff.
4. Existing contracts, licences and outsourcing arrangements

The University has a small number of contractual and other arrangements in place which may involve access to or use of personal information held by QUT. Typical contracts and arrangements are for:

- provision of information to prospective students;
- use of mailing houses to send material such as enrolment materials, election papers, promotional publications or information on QUT services to students, other clients of the University or alumni;
- engagement of external organisations to undertake database verification and relationship building in relation to QUT alumni and supporters;
- provision of training to staff and students of overseas institutions in accordance with Memoranda of Understanding;
- storage of staff and student files off-campus; and
- maintaining contact with and organising functions for overseas alumni of QUT.

These arrangements generally place requirements on contractors or service providers for the maintenance of the confidentiality of any personal information which is provided for the limited purpose of the provision of the service. As these contracts expire or are renewed, any new arrangements will ensure compliance with the requirements of IS42.

5. Responsibility for privacy at QUT

Overall responsibility for privacy at QUT rests with the Vice-Chancellor as Chief Executive Officer. Whilst all staff of QUT have a general responsibility to comply with QUT’s Privacy Policy (MOPP F/9.1), responsibility for general management of privacy requirements at QUT has been delegated to a Privacy Contact Officer, the Corporate Information Coordinator who is based in the Secretariat. The Privacy Contact Officer is the first point of contact for students, staff and clients of the University on privacy matters, including general information about privacy obligations and QUT’s policy on information privacy, requests pursuant to IPPs 6 and 7, and for advice on breach of privacy complaints.

Contact details are:

Corporate Information Coordinator
(QUT Privacy Contact Officer)
Secretariat
U Block, Gardens Point Campus

GPO Box 2434
Brisbane Qld 4001

Telephone (07) 3864 1911
Facsimile (07) 3864 1818

Email privacy@qut.edu.au
6. Implementation

QUT has implemented the requirements of IS42 through:

- review and update of QUT’s policy on information privacy to reflect the introduction of IS42, and analysis of related policies for consistency;
- development of a privacy and security statement for the QUT website;
- development of IPP 2 notices in respect of the information which we collect directly from students, staff and other clients;
- analysis of existing arrangements for protecting personal privacy in human research;
- development of model contractual terms compliant with IS42 requirements;
- development of an annual program of training and awareness-raising for staff at all levels.

Current activities associated with the ongoing development and improvement of the University’s privacy framework include:

- review of the University’s staff Code of Conduct to include a statement on privacy;
- identification of activities where privacy issues have impact on action to be taken and development of supporting guidelines and protocols;
- monitoring and training; and
- annual review and update of privacy plan and policy.

7. Access and amendment procedures (IPPs 6 and 7)

IPPs 6 and 7 recognise that privacy rights and principles include rights of access to and amendment of personal information. IS42 refers specifically to the existing rights of access and amendment of personal affairs information under the Queensland Freedom of Information Act 1992 (the FOI Act). The provisions of the FOI Act confer a right on individuals to obtain access to documents concerning their personal affairs without incurring any fees or charges. In addition, the FOI Act enables individuals to seek amendment of their personal affairs information if they believe it is inaccurate, incomplete, out-of-date or misleading. “Personal affairs” information has a narrower meaning that “personal information”, and refers only to information concerning private aspects of a person’s life.

7.1 Access arrangements at QUT

QUT is committed to providing, as far as practicable, an open environment which enables members of the public and the QUT community to access University documents without recourse to formal procedures under the FOI Act.

To achieve this, QUT has in place arrangements whereby members of the University staff may inspect their personnel records by arrangement with Human Resources Department staff. Students may inspect their student records by arrangement with the Student Business Services Department. Persons who have been unsuccessful in applying for appointment to QUT may also obtain information concerning their application and the selection process by contacting the Human Resources Department. Individuals seeking access to other types of personal records which the University holds about them should contact the Privacy Contact Officer in the first instance, who
will assist with making a request to the appropriate organisational unit or arrange access where necessary.

It is recognised that, on occasion, it will be necessary or appropriate to make an application under the FOI Act to the FOI Officer, for instance, where documents are considered exempt from access or where consultation with third parties may be necessary. The Privacy Contact Officer also acts as QUT’s FOI Officer and is able to advise in these situations.

7.2 Requests for amendment of information

QUT has a similar approach to the rights of amendment of personal information in the FOI Act. In simple cases, where evidence is given, an appropriate officer of the University may alter the record without using the formal FOI mechanisms. In more complex cases (eg where opinion or other interpretative information is involved, or if a determination needs to be made as to whether personal affairs information is involved), it will be necessary to make application to the FOI Officer.

7.3 Further information

Where an FOI application is necessary or to obtain further advice on FOI processes, contact the Corporate Information Coordinator, who acts as QUT’s FOI Officer. Contact details are found in section 5.

QUT’s approach to information access and privacy is articulated in the Privacy Policy (MOPP F/9.1), and in the Freedom of Information Policy (MOPP F/10.1), at www.qut.edu.au/admin/mopp/.

8. Privacy complaints

If an individual believes that QUT has not dealt with their personal information in accordance with an IPP, they may make a complaint in writing to QUT. A complaint must be made in writing within six months from the date when the breach of the IPP was suspected to have occurred. Written complaints should be sent to the Privacy Contact Officer, at the address listed in section 5 above. The Privacy Contact Officer (telephone (07) 3864 1911) can provide more information about complaint handling procedures.

Complaints will be acknowledged by the Privacy Contact Officer in writing within 14 days from the date upon which the written complaint was received. The Privacy Contact Officer will refer the complaint to the head of the organisational unit having responsibility for the personal information to which the complaint relates. Primary responsibility for investigating and responding to the complaint will rest with the head of the organisational unit, who will provide a written response to the complaint within 60 days of the date upon which it is received. The response will advise of the conclusions reached following investigation of the complaint and any action that will be taken for resolution.

If a complainant does not agree with the University’s response, they can apply in writing to the Registrar for an internal review of the response to the privacy complaint. Applications for internal review must be made within 28 days of the complainant receiving the initial notification on the complaint. The postal address for internal review applications is:
Registrar
Queensland University of Technology
GPO Box 2434
Brisbane Qld 4001

The internal review will be completed within 60 days of receipt of the application for internal review. The Registrar will provide a written response to the individual who has requested internal review.
Appendix 1 – Information Privacy Principles (From Information Standard 42)

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.

**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.
Information Privacy Principle 6

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.

Information Privacy Principle 7

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
   (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.

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.

---

1This 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.

2This 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.
**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.