



PUBLIC TRUST OFFICE PRIVACY PLAN 2008-2009

Contents

Introduction	2
Personal Information	2
Information Privacy Principles (IPPs)	2
Privacy & the PTO	3
Acts Administered by the PTO	3
Nature, purpose & classes of personal information held by the PTO	
Employee and corporate support records containing personal information.....	3
Business and service delivery records containing personal information	4
Contractual arrangements with external bodies	5
Public Registers managed by the PTO.....	5
How long each type of record is kept	6
Privacy codes of practice	6
Implementation of the privacy plan	7
Implementation steps	7
Current practice.....	7
Collection and storage of personal information (IPPs 1 to 4).....	7
Access to and alteration of personal information and the Privacy Plan (IPPs 5, 6 and 7)	8
Accuracy, use and disclosure of personal information (IPPs 8 to 11)	8
Complaints about breaches of the IPPs.....	8
Training.....	8
Privacy Contact Officer’s responsibilities	8
Procedures to Gain Access or Amend Personal Information	9
Privacy Review Procedures	10
Appendix A	12
The Information Privacy Principles	
Information Privacy Principle 1.....	12
Information Privacy Principle 2.....	12
Information Privacy Principle 3.....	12
Information Privacy Principle 4.....	12
Information Privacy Principle 5.....	13
Information Privacy Principle 6.....	13
Information Privacy Principle 7.....	14
Information Privacy Principle 8.....	14
Information Privacy Principle 9.....	14
Information Privacy Principle 10.....	14
Information Privacy Principle 11.....	14
Appendix B	15
Employee records containing personal information	15
Financial management system personal information.....	15
Information systems personal information	16

Public Trust Office Privacy Plan 2008-2009 Information Standard 42

Introduction

The Queensland Government has developed a privacy policy that applies to the Queensland public sector. The privacy policy requires personal information held by Queensland Government agencies to be responsibly and transparently collected and managed in accordance with 11 Information Privacy Principles (IPPs).

The privacy policy is not contained in legislation but has been introduced administratively through an Information Standard 42 (IS 42) which contains the IPPs. IS 42 and the IPPs can be accessed at <http://www.iie.qld.gov.au/informationstandards/downloads/IS42.pdf>.

IS 42 requires each agency to prepare a privacy plan which is approved by the Chief Executive Officer of each agency. IPP 5 sets out what the plan must contain.

The purpose of The Public Trust Office's Privacy plan is to provide:

- The public with details about the types of personal information held by the Public Trust Office ["PTO"];
- Individuals with details about how they can access their personal information that is held by the Public Trust Office;
- Details of how the Public Trust Office will implement the privacy policy; and
- Guidance to Public Trust Office staff who deal with personal information.

Personal Information

The privacy policy applies to the collection, management and use of personal information. IS 42 defines "personal information" 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."

The information does not have to clearly identify a person. It only needs to provide sufficient information to lead to the identification of a person. It is not limited to confidential or sensitive personal information. Examples of personal information include a person's name, address, date of birth or phone number. IS 42 covers information held in paper or electronic records and may extend to body samples or biometric data.

Information Privacy Principles (IPP's)

The 11 IPPs are a set of directions that Government agencies must adopt and follow when collecting, handling, using and disclosing personal information about people mentioned in the Public Trust Office's records. The full text of the IPPs is set out in *Appendix A*.

IPPs 1, 2 and 3 deal with what personal information may be collected, the way it is collected and what notices must be given to the person from whom the information is collected.

IPPs 4 and 5 deal with requirements for ensuring that personal information is stored securely and protected from loss, unauthorised access, use, modification, disclosure or misuse.

IPPs 6 and 7 deal with individuals obtaining access to and correcting the personal information held by departments and agencies.

IPPs 8, 9, 10 and 11 deal with how personal information is used and disclosed by departments and agencies.

Privacy & the PTO

The Public Trust Office is committed to protecting user privacy. We understand that clients of the Public Trust Office are concerned about their privacy, and the confidentiality and security of any information that is provided.

Section 15 of the **Public Trustee Act 1978** prescribes that:

“Every member of the staff of the Public Trust Office, every agent of the public trustee and every member of The Public Trust Office Investment Board constituted pursuant to section 21 shall be bound to secrecy by declaration in the form approved by the public trustee.”

The practices and procedures of the Public Trust Office also comply with the requirements of the **Trusts Act 1973**, the **Succession Act 1981** and other legislation which impose obligations and duties on trustees, executors, attorneys and administrators.

Acts Administered by the PTO

Public Trustee Act 1978

Note: Access to information is subject to the provisions of the **Freedom of Information Act 1992** and the **Public Records Act 2002**.

Nature, Purpose & Classes of Personal Information Held by the PTO

The Public Trust Office holds electronic and paper records containing personal information, which can broadly be divided into two classes:

1. records relating to staff employment and corporate support; and
2. records relating to the performance of the Public Trust Office’s business and service delivery functions.

Employee & Corporate Support Records Containing Personal Information

Most of the records held in the Human Resources Management unit are records relating to some aspect of staff employment. The biggest electronic database containing staff personal information, “Aurion”, is used for a number of purposes including payment of salaries and recording information about staff such as service history and qualifications. “Aurion” also prepares reports for Government purposes relating to staffing.

Staff records are also held in the business or service delivery areas. These records remain in that area for as long as the staff member works there, and include records such as time sheets and performance, planning and review documents.

A list of generic classes of personal information about staff relating to all aspects of employment is set out in *Appendix B*.

Business and service delivery records containing personal information

The Public Trust Office performs diverse functions and holds a substantial amount of personal information in its records about a large number of people obtained in the ordinary course of performing the functions of the Office. All areas may hold some records containing personal information related to the performance of their respective functions. The major business and service delivery areas of the Department are:

- Administration of Deceased Estates
- Administrator under appointments by the *Guardianship and Administration*
- Charitable Trusts
- Conveyancing, Gladstone & Mt Isa areas
- Custodial and securitisation services
- Enduring Powers of Attorney
- Establishment and management of trusts
- Investment services & products
- Personal financial management and advocacy (particularly for people with a disability)
- Property, jewellery & motor vehicle auctions
- Safe custody of wills & other important documents
- Taxation services
- Trustee of unclaimed money, property & superannuation

To enable the Public Trust Office to provide these services it is necessary to collect, store and use a variety of information.

- ◆ Client personal information is required in the delivery of the services detailed above. It is necessary to record personal information of clients to provide these services to clients. The client personal information is retained for the periods prescribed by the various laws which apply to the services provided by the Public Trust Office and the ***Public Records Act 2002***.

The majority of client personal information is retained in Public Trust Office computer systems. The access rights of staff, agents and contractors are strictly limited to the parts of the computer systems that are necessary for them to carry out their duties or contractual obligations.

- ◆ Personal information about vendors and contractors to allow normal business processes to take place; e.g. name, address for payment, bank account details to allow for electronic payment of accounts. This information is retained for the periods prescribed by the various laws which apply to the services provided by the Public Trust Office and the ***Public Records Act 2002***. The access rights of staff, agents and contractors are strictly limited to the parts of the computer systems that are necessary for them to carry out their duties or contractual obligations.
- ◆ Employee personal information which is required so that human resource management functions, including recruitment, can be carried out. This information is retained various periods as specified in the policies, standards and guidelines

about the making, keeping, preserving, managing and disposing of records by the State Archivist under s.25 of the *Public Records Act 2002*.

- ◆ The access rights of staff, agents and contractors to employee personal information are strictly limited to the parts of the records and computer systems that are necessary for them to carry out their duties or contractual obligations.

Contractual arrangements with external bodies

The Public Trust Office enters into contractual arrangements with external bodies for the supply of goods and services. In many cases the agreements extend over several years. Many were in existence before the Department was required to comply with the privacy principles in contractual arrangements with external bodies. Many of the contracts containing personal affairs information concern staff issues including private sector consultancies.

Existing contracts will be reviewed and where possible, altered to comply with the relevant privacy principles. As the current contracts and agreements expire and are replaced or renegotiated they will incorporate the express reference to requirements of the IPPs.

Public Registers Managed by the PTO

The Public Trust Office maintains the unclaimed monies register as prescribed by s.99A of the *Public Trustee Act 1978*.

The Public Trustee receives unclaimed money and unclaimed property in Queensland from a variety of sources. These include:

- **Companies:** Where dividends or other monies have been held for two years for shareholders who cannot be located, a company is required to maintain a Register of those unclaimed monies. Any money on the Register which is still unclaimed after a further year must be paid to the Public Trustee.
- **Unclaimed Superannuation:** Where a Superannuation member turns pensionable age and the Superannuation Fund has been unable to locate such member or on the death of a member and benefits have not been claimed by an Executor or Administrator such benefits must be paid to the Public Trustee.
- **Hospitals and Institutions:** Hospitals and Institutions are required to deliver to the Public Trustee any property including jewellery, money which has remained there unclaimed for three months or more.
- **Missing Persons and Unknown Owners:** If a person goes missing or the owner of property cannot be found or is unknown, such property can be administered by the Public Trustee.
- **Deceased Estates:** If a beneficiary cannot be located or it cannot be established who is entitled to benefit, the share or whole estate is held as unclaimed.
- **Trustees:** Any Solicitor, Public Accountant, Real Estate Agent, Auctioneer or Agent who operates a Trust Account in Queensland and who has in their possession money or property on behalf of a beneficiary
 - whose identity is not known
 - whose whereabouts are unknown
 - whether he or she is alive or dead is unknown
 - if deceased and their executors or administrators are unknownare required after a certain time to pay such money to the Public Trustee.

- **Local Authorities:** Local Authorities have the power to sell freehold property when rates and charges remain unpaid for three years. After deducting sale expenses and the rates owing, Local Authorities are required to pay any balance, which remains unclaimed for two years to the Public Trustee.
- **Residential Tenancies:** If a tenancy agreement is terminated and goods or personal documents are left on the property it is necessary for the landlord to follow certain procedures and account to the Public Trustee.
- **Pawnbrokers:** Pawnbrokers are to forward the net proceeds of sale of unredeemed pledges.
- **Uncollected Goods:** A trader may transfer these to the Public Trustee.
- **Unclaimed Repairs:** A repairer is entitled to sell items left but never claimed, deduct expenses, and pay the net proceeds of sale to the Public Trustee.
- **Unclaimed Prizes:** Unclaimed winnings in art unions and similar organisations are paid or transferred to the Public Trustee.

Access to details in the above registers is restricted to the purpose for which the register is kept.

In 2004 an online Unclaimed Moneys search and lodgement facility was released to meet the needs of those in the community searching for Unclaimed Moneys and those in the business community who are required to lodge Unclaimed Moneys and Unclaimed Superannuation with the Public Trustee of Queensland. The Unclaimed Monies search facility can be accessed at:

<http://www.pt.qld.gov.au/services/unclaimed/index.asp>

The contact officer details for the unclaimed monies register is:

Unclaimed Moneys Officer
Ph: **32139368**
Fax: **32139471**
E-mail: unclaimedmoney@pt.qld.gov.au
Address: Unclaimed Moneys Officer
Public Trustee of Queensland
PO Box 1449
BRISBANE Qld 4001

How Long Each Type of Record is Kept

The disposal of PTO records is governed by the *Public Records Act 2002*(the Act). Under the Act a record cannot be disposed of without an authority from the State Archivist or other legal authority. PTO records are kept for varying periods in accordance with the Act and the General Disposal and Retention Schedule for Administrative Records issued under that Act.

Privacy Codes of Practice

IS 42 permits agencies to develop privacy codes of practice. A privacy code of practice is a statement of how a public sector agency will perform a specific function and may modify the application of any one or more of the IPPs for that purpose. Although, the Public Trust Office has not established any codes of practice for performing its obligations, the issue of the need for a code of practice is under review.

Implementation of the Privacy Plan

The Public Trust Office Privacy Officer has coordinated the delivery of information about the IPPs to Office staff. However, **business managers** and **directors** are responsible for putting systems into place within their management area to ensure compliance with IS 42 and the IPPs.

All Public Trust Office staff have received training in the application of the IPP's and the effect of this privacy plan.

All business managers and directors must ensure that the staff in their respective areas of responsibility know about the Public Trust Office's responsibilities for the retention, storage and disposal of departmental records and ensure that these responsibilities are complied with in relation to IS 42 and the IPPs.

All staff have received training on their privacy obligations and responsibilities in complying with the requirements of IS 42 and related guidelines. Information is regularly provided to all staff to ensure that they are aware of the requirements of IS 42 and the IPPs. **Line managers** are responsible for changing their work systems to comply with the IPPs.

This privacy plan is reviewed annually.

Implementation Steps:

Staff are encouraged to be pro-active in implementing privacy. Some of the steps that managers and directors were requested to undertake to implement privacy, are set out below. They are not exhaustive.

Current practice

- Assess current practice and procedure. This can be done by auditing records to identify those containing personal information.
- Review the purpose and functions for which the information is held.
- Ascertain whether exemptions apply, refer to relevant law to ascertain the applicability of the law and identify risk or exposure to application of the IPPs and the potential for breach.

Collection and storage of personal information (IPPs 1 to 5)

- Review the purpose for which the information is obtained and ensure collection is lawful and directly relates to a function or activity of the area of the Office.
- Review forms used to collect personal information from clients and employees.
- Ascertain what people are informed of when personal information is obtained, if consent to disclosure is required and whether notification requirements are met.
- Assess whether people who collect information by phone are equipped to inform clients about the Office's obligations under the IPPs.
- Assess what quality control measures are needed to be put in place.
- Assess the adequacy of information given to people at the point of collection of personal information.
- Review policies and practices for secure storage of personal information held in records (paper or electronic or otherwise).

- Assess whether storage security is sufficient.
- Assess who within the Office has access to personal information about other people and whether any limitations are desirable or necessary.
- Assess compliance with and the adequacy of retention and disposal requirements and methods of disposal.

Access and alteration of personal information (IPPs 6 and 7)

Ensure staff know that access to and alteration of personal information is to be dealt with under the *Freedom of Information Act 1992* and that when a written request for access or alteration is made, it is sent to the Freedom of Information Co-ordinator.

Accuracy, use and disclosure of personal information (IPPs 8 to 11)

- Assess the quality and accuracy of information collected and retained for Office use.
- Ascertain what procedures are in place to ensure personal information is accurate, up to date and complete before it is used. Assess what quality control measures are needed.
- Review systems to minimise errors or misinterpretation of personal information, to ensure that standards are adopted for lawful, consistent, accurate use and transfer of information about people between areas of the Office and to other agencies.
- Ascertain whether personal information is being used only for the purpose for which it is collected.
- Ascertain what personal information staff disclose.
- Ascertain whether there is proper authority for disclosure and that procedures are put in place to ensure that the proper authority is obtained before a disclosure is made.
- Develop appropriate policies and procedures and assess the appropriate quality control measures to be put in place.
- Ascertain whether personal information disclosed for research purposes contains information which could lead to the identification of people whether living or dead.

Complaints about Breaches of the IPP's

Assess procedures in place for dealing with receiving complaints from the public about breaches of the IPPs and the investigation of complaints.

Training

Assess the training requirements that will be necessary to ensure that staff are informed, and kept regularly informed, of the requirements of IS 42 and the IPPs as they apply to each officer's work.

Privacy Contact Officer's responsibilities

The Department's goal is to fully implement the privacy plan by September 2003. The steps to implement the plan are set out below. Informing staff of their privacy obligations and responsibilities will be critical in ensuring that the Department complies with the requirements of IS 42.

Action	Implementation Plan
Staff awareness of privacy responsibilities	Inform staff of the content and implementation steps for the privacy plan. Develop and place a privacy and security statement on the website. Assist in the review and update PTO administration manuals to include privacy.
Provide training on privacy Issues	Provide privacy training for executive management, managers and Office staff. Develop handout for inclusion in new staff induction kits.
Review contracts	Review contracts and license agreements for compliance with the IPPs.
Review relevant policies/guidelines	Assist in the review of policies and guidelines for to integrate privacy issues where appropriate. Assist in the review and upgrade grievance procedures to include privacy complaints. Assist in the review and upgrade procedures for dealing with transfer of information within the Office and to other agencies
Develop complaint handling procedures	Assist in the development of guidelines and procedures on complaint handling and resolution. Review all notices, applications, forms, questionnaires etc.
Review of all notices, forms, questionnaires etc	Assist in the review of all notices, forms, questionnaires etc to ensure compliance. Modify where necessary.
Develop privacy policies and guidelines	Assist in the development of guidelines to be given to contractors regarding privacy responsibilities. Review and upgrade terms of contracts to progressively accommodate privacy compliance. Assist in the development of guidelines for application when personal information is collected. Assist in the development of guidelines for staff with special responsibilities for personal information (eg: human resources, counselling, health and safety, employment and service equity). Assist in the development of guidelines for staff generally regarding privacy responsibilities.
Conduct annual review	Review and update privacy plan.
Monitor privacy awareness	Conduct periodic surveys to monitor understanding of and compliance with privacy principles.

Procedures to Gain Access or Amend Personal Information

At the Public Trust Office, decisions and actions taken may be made on the basis of personal information in our possession. Therefore, it is important that your personal information is accurate, complete, and up to date. You are therefore welcome to access and verify the information we have about you.

The first step is to request access to the information through your usual the Public Trust Office contact, e.g. Trust Officer, Wills Officer, Property Officer, Financial Services Officer, Human Resource Officer. We may ask you to put your request in writing and supply appropriate identification. If the request fulfils the outlined requirements, we will give you access to the

information in a mutually agreed format (in many cases this will be by directly viewing the original, or a copy, of the documentation on file).

If you believe that any part of the information is not accurate or complete, you can request us to amend it accordingly. Again, we may ask you to put your request in writing. If we are reasonably satisfied that our records need amendment, we will make the amendment as soon as possible. If we do not agree that our records need amendment, we will inform you of the reason(s) and you may require us to keep a statement on our records that you believe the information is not accurate, complete or up to date.

There is no charge for an individual to seek access to or apply to amend their personal information. However, your right of access to and amendment of personal information is subject to exceptions provided in the ***Freedom of Information Act 1992*** or any other State Law.

Please note that before providing you with any of your personal information we will ask you to provide evidence of your identity. If it is determined that you are required to lodge a formal application under the ***Freedom of Information Act 1992***, you must make an application in writing. An application must:

- be in writing;
- state an address to which a notification of the decision may be sent;
- be accompanied by a **\$38.00** application fee, if the information relates to non-personal matters (personal information about yourself is available at no cost); and
- be addressed to the Freedom of Information Officer.

Post the application to: **The Freedom of Information Officer
Public Trust Office
GPO Box 1449
BRISBANE QLD 4001**

or deliver the application to: **The Freedom of Information Officer
Public Trust Office
Level 12
444 Queen Street
BRISBANE QLD 4000**

or for further information contact the Freedom of Information Officer on:

**Telephone (07) 32139337
Facsimile (07) 32139486**

* ***NOTE: In addition, other charges [e.g. \$23.20 per hour processing costs and 20 cents per page photocopying charges] may apply and you may be required to pay a deposit. A statement of any charges will be supplied to you. You will be notified of the decision on access to documents before full payment is required.***

Privacy Review Procedure

If an individual believes that their personal information has not been dealt with in accordance with an IPP they may make a complaint to the Public Trust Office seeking an internal review. A request for an internal review must be made in writing and must be made within six months from the date when the breach was suspected to have occurred.

Requests should be forwarded to:

**Mr Glenn Dickson,
Privacy Contact Officer,
GPO Box 1449,
Brisbane Qld 4001,**

or faxed to: **07 32139486**


or e-mailed to: ***glenn.dickson@pt.qld.gov.au***

Requests for review will be acknowledged in writing within 14 days from the date on which the application was received, and the agency will process the request within 60 days from the date on which the application was received. Applicants will be advised in writing of the agency's decision.

If an applicant does not agree with the Public Trust Office's decision they may request an internal review.

Applications for review should be made within 28 days of the complainant receiving the initial complaint decision. Applications for review should be sent to the Privacy Coordinator at the address outlined above. The review will be carried out by a person who has not previously been involved in the matter and who is more senior than the person who made the initial decision. The review will be completed within 28 days of receipt of the application for review. The complainant will be notified in writing of the outcome of the review.

I approve the *Public Trust Office Privacy Plan 2008-2009*.


**Patrick Wedge
Acting Public Trustee**

26 11/2008

Appendix A

The Information Privacy Principles

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 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 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.

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.

Appendix B

Employee records containing personal information

The various management areas of the Public Trust Office hold types of employee records in common with each other which contain personal information about current and past staff. The purpose of these personnel records is to maintain employment history, payroll and administrative information relating to all permanent, contract and temporary staff of the Public Trust Office. Recruitment, personnel and payroll records containing personal information may include records concerning:

- attendance at work and overtime
- leave applications and approvals
- medical matters
- payroll and pay matters, including banking details
- tax file numbers
- declarations of pecuniary interests
- personal histories
- performance appraisals
- personal development and training
- trade, skill and aptitude tests
- work related travel
- personal welfare matters
- contracts and conditions of employment
- recruitment, relocation of staff and removal of personal effects
- character checks and security clearances
- work related accidents and injuries
- compensation matters
- rehabilitation matters
- discipline matters
- counselling matters
- allegations and investigation of alleged misconduct
- criminal convictions
- complaints and grievances
- recommendations for honours and awards

Specific personal information held for each employee includes name, address, date of birth, occupation, employee identification number, gender, qualifications, equal employment opportunity group designation, citizenship details, next of kin, details of pay and allowances, leave details, time sheets and security clearance details.

Current and former employees and other people (for example, spouses and next of kin who believe that the Public Trust Office's personnel records may also contain personal information about them) can obtain information regarding access to their personal information by contacting the Manager, Human Resources on ph. 32139223 or the Public Trust Office's Freedom of Information Co-ordinator on ph. 32139337.

Financial management system personal information

The purpose of these records is to process and account for Public Trust Office's expenditure and revenue in the conduct of its business and service delivery. The content of these records may include name, address and service provided or goods delivered. The records include personal information about creditors, debtors, and out sourced services and service providers.

If the service provided or goods delivered concerns or mentions a particular person or group of people, that personal information may also be included in these records.

Accounts staff have access to financial records. This information is not usually disclosed to other persons or organisations unless there is a specific legislative requirement which requires or authorises disclosure.

Individuals can obtain information regarding access to their personal information by contacting the Chief Finance Officer on ph. 32139314.

Information systems personal information

Public Trust Office's information technology (IT) system routinely carries information about the core business and the corporate services of the Public Trust Office. It encompasses both internal electronic transactions and external transactions, including telephone, e-mail, internet and government intranet activity.

There are some personal information records specifically tailored to IT system administration. This includes IT system security identifiers and usage tracking records about staff users of the IT system that are held by central IT administrators and staff supervisors.

The information is not disclosed to persons other than staff supervisors, system administrators and the individual officer concerned unless a specific legislative requirement requires or authorises access or disclosure.

Individuals can obtain information about access to their personal information by contacting the Chief Information Officer on ph. 32139465.