The Public Trustee

Information Privacy Plan

February 2015

Approved

Name	Title	Signature	Date
Mark Crofton	A/Public Trustee of Queensland	FILE COPY SIGNED	12/03/2015

Endorsed

Name	Title	Signature	Date
Kathryn Williams	A/Official Solicitor	FILE COPY SIGNED	26/02/2015
Caroline Hannigan	Director Governance and Executive Directorate	FILE COPY SIGNED	26/02/2015
Tony Steinmetz	Executive Director Client Services	FILE COPY SIGNED	10/03/2015
Tim Murphy	Executive Director Investment Services & CFO	FILE COPY SIGNED	06/03/2015

Contact Details

Owner:	Governance & Executive Directorate
Contact Details:	07 3213 9172
Program Name:	Governance and Executive Directorate
Document Status:	Review
Document Location:	G:\Governance & Executive Directorate\Corporate Governance\Information Privacy \ Information Privacy Plan 4.0

Revision History

Revision Date	Version No.	Author	Description of Change/Revision
28 Oct 2011	0.1	Ralph Sadler	Created first version
14 Nov 2011	0.1.2	Ralph Sadler	First draft circulated for feedback
4 Jan 2012	1.0	Ralph Sadler	Final for approval
17 Dec 2012	2.0	Wayne Batts	Incorporate review changes
7 Jan 2013	3.0	Sanjana Matheson	Incorporate review changes
June 2014	4.0	Joseph Maurirere	Incorporate review changes
August 2014	5.0	Joseph Maurirere	Incorporate OIC suggestions

Contents

1. Introduction

The *Information Privacy Act 2009* (IP Act) regulates how the Queensland public sector manages personal information. It creates an obligation to comply with the privacy principles, which include the Information Privacy Principles (IPP) the National Privacy Principles (NPP), the conditions under which personal information may be transferred outside of Australia and the rules regarding contracted service providers. Chapter 3 of the IP Act creates a right for individuals to access and amend their personal information.

The NPPs only apply to health agencies. Queensland Government agencies including The Public Trustee of Queensland (Public Trustee) are required to comply with the IPP.

In delivering our services to the people of Queensland we collect personal information from our employees, clients and members of the public. The Public Trustee values the importance of the privacy of individuals and understands the need to act responsibly and transparently when collecting and managing this information.

The aim of this Plan is to assist employees, clients and members of the public to understand how we manage personal information in accordance with the IP Act. This document is to be read in conjunction with the Privacy Information Digest which outlines the types of personal information we collect, use, store and disclose.

2. Privacy responsibilities

The overall responsibility for privacy in our organisation rests with the Public Trustee of Queensland. Employees are responsible for compliance with the IP Act.

Any employee may be asked about privacy matters and so should be familiar with our Information Privacy Policies and procedures. Simple enquiries can be dealt with by reference to the Privacy page on the Public Trustee website at http://www.pt.qld.gov.au/about-us/privacy.html.

Responsibility for overall privacy compliance is a function of the Governance and Executive Directorate (GED). The directorate is the primary contact for the following matters:

- compliance with and general information about information privacy;
- liaison with the Department of Justice and Attorney General (DJAG) Right to Information; (RTI) & Privacy Unit for processing of Access Applications made under the IP Act;
- requests to amend records containing personal information under the IP Act; and
- suspected breaches of privacy and privacy complaints.

For further assistance and advice please contact the Governance Officer on (07) 3213 9172 or via email governance@pt.qld.gov.au

3. Application of this plan

This Plan applies to all temporary and permanent full-time and part-time employees.

4. Personal information

4.1 What is personal information?

Personal information is defined in the IP Act at section 12 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."*

Personal information can include correspondence, audio recordings, images, alpha-numerical identifiers and combinations of these, such as a birth certificate.

Information does not have to be true in order to be personal information and it does not need to be written down or recorded in another material form, such as a photograph or audio recording. It can be spoken or communicated in another way, for example, by sign language.

In order to be considered ‘personal information’, two criteria must be satisfied:

- the information must be about an individual; and
- the individual’s identity must be reasonably ascertainable from the information or opinion.

The information does not have to clearly identify a person. Information can be personal information even if an individual’s identity is not immediately apparent, as long as their identity can be reasonably ascertained by reference to other information.

Examples of personal information include a person’s:

- name
- residential address
- email address
- signature
- date of birth
- driver’s licence number
- employee number
- physical description such as height, tattoos
- photograph
- political and religious beliefs
- medical records
- disabilities
- sexual preference

Electronic and hard copies of records we hold containing personal information can be classified into two categories:

- employees and corporate support; and
- performance of business and service delivery functions.

4.2 What is not personal information?

Information about an anonymous individual or information that cannot be used to reasonably ascertain the identity of an individual is not covered by the IP Act.

The definition of personal information limits it to information about an individual. The definition of 'individual' in the *Acts Interpretation Act 1954* (Qld) is 'a natural person'. A natural person can only be a living person. This means that deceased people cannot have personal information; however care should still be taken when handling the information of the deceased, as it may also be the personal information of the living, for example, a family member.

Businesses and community organisations do not have personal information.

The collection principles do not apply to personal information in publications that are generally available, such as magazines, books, newsletter or newspaper articles, annual reports, internet publications and the Queensland Government Gazette. If that personal information appears in a record of the agency, then the IPP will apply.

5. Privacy Principles

The IP Act contains the following Privacy Principles which all Queensland state agencies, except for health agencies, must comply with:

- 11 Information Privacy Principles (IPP);
- Overseas Transfer Principles; and
- Contracted Service Provider Principles.

These principles cover the collection, storage, use and disclosure of personal information. Many of the principles only require that reasonable steps be taken having regard to the circumstances.

The purpose of the 11 Information Privacy Principles (IPP) in schedule 3 of the IP Act is to:

- regulate the way Queensland government agencies are to collect, store, and secure personal information;
- limit the circumstances in which personal information can be used and disclosed;

- allow individuals to request access to information agencies keep about them and/or amendments to this information if it is incorrect; and
- require agencies to take steps to assure the quality and accuracy of personal information prior to using it.

6. Compliance with Privacy Principles

This section documents our various systems, policies and procedures established to comply with the IP Act.

6.1 IPP 1 – 3: Collection of personal information

6.1.1 Relevant and Lawful

Personal information is only to be collected where it is required to fulfil a lawful purpose directly related to a service we deliver. It is not to be collected for personal use or other purposes.

An agency must have a specific purpose in mind when collecting personal information, and must not collect any more than is necessary. An agency must not use unfair or unlawful means of collection. However, where we are collecting information to fulfil our obligations as financial administrator we may have to collect information to fulfil a future function or activity. In these limited circumstances, the collection of personal information is necessary to fulfil a lawful purpose such as full or limited financial administration of a person's affairs. In these circumstances the individual providing the information will be advised.

6.1.2 Unsolicited information

In instances where we receive more personal information than required to provide a service the IPP still apply.

6.1.2.1 Collection notices

Before collection of personal information or as soon as practicable afterwards, the person providing the information is to be advised about:

- the purpose of the collection;
- any law authorising the collection; and
- to whom we would normally disclose information and, if known, anyone they in turn will disclose it to.

In addition to the generic collection notice published on our website, every collection form and tool is to include a specific collection notice tailored to that collection activity. Where personal information is collected face-to-face or via telephone the collection notice may be given verbally at the time of collection and this notification recorded on file. Personal information is only to be collected using tools and forms approved by Governance & Executive Directorate to ensure compliance with the Privacy Principles.

6.2 IPP 4: Storage and security of personal information

6.2.1 Protection

Employees are to comply with the IP Act and all internal Information Privacy policies and procedures to ensure documents containing personal information are protected from loss, unauthorised access, use, modification or disclosure and any other misuse. Managers are responsible for ensuring staff know and apply the physical, electronic and operational security measures that apply to their work groups.

Records must not be kept any longer than the intended minimum retention period and must be disposed of appropriately and in accordance with our Queensland Governments General Retention and Disposal Schedule for Administrative Records and the Public Trustees Retention and Disposal Schedule.

The level of storage and security will depend upon the nature of the personal information and the risk of a security breach occurring as determined by the Public Trustee's Chief Information Officer.

6.2.2 Electronic and physical access

Access to personal information stored on our electronic systems and held in hard copy in physical containers is only to be granted to employees needing access to perform their duties.

Employees are authorised to access only the minimum personal information needed to fulfil their duties. Employees are not to access personal information, held on electronic systems or hard copy records, for purposes other than those directly related to the purpose for which the information was collected. Managers are to ensure that internal electronic and physical security procedures are understood and followed by staff.

Audit logs are maintained on all electronic systems for monitoring and review by Internal Audit to ensure compliance with electronic access policies and procedures.

6.2.3 Public Trustee website – Publishing Personal Information

An individual's personal information is not to be published on our website unless there is a business reason to do so and consent has been given by the individual concerned.

Section 33 of the IP Act sets outs the circumstances in which an agency may transfer personal information out of Australia. Any transfer of personal information must comply with these rules or the transfer will be a breach of the obligation to comply with the privacy principles.

The act of making personal information available on the Public Trustee website will not amount, in and of itself, to a transfer of the personal information out of Australia, as long as the web server on which the webpage is stored is in Australia.

However, because of the way the World Wide Web works, as soon as someone from another country accesses the personal information on the website, a copy of that webpage will be transferred out of Australia. This means that any personal information placed on the Public Trustee's website is potentially going to be transferred out of Australia—all it takes is someone from another country to access it.

6.2.4 Social media

Employees are not to publish or store personal information in possession of, or controlled by Public Trustee on their personal social media accounts or online services.

6.2.5 Emailing personal information

Unless approved by management, employees are not to send personal information in the possession or under the control of the Public Trustee, by email under any circumstances. This includes sending personal information to the person it concerns and to the employee's home email address to work on that information on their personal computer.

6.2.6 Portable Computers and Portable Storage Devices (PSD)

PSD are small, lightweight, portable devices capable of storing large amounts of data. For the purpose of this plan, PSD include the following:

- Laptops, Tablets (iPad etc.), notebooks;
- USB memory stick or flashdrive and portable external hard drives;
- Personal Digital Assistants (PDA);
- Smart Phones (e.g. iPhone, Blackberry etc.); and
- MP3 players with data storage capabilities.

If required for specific business purposes, Information Services will issue a PSD from a central pool. Personal information in our possession or under our control is not to be stored or processed on employees' private PSD. Only Executive Directors, Directors and Regional Managers are to be issued with a PSD. Where a Universal Serial Bus (USB) memory stick is used to collect, use, store

and disclose personal information, these devices should be encrypted to ensure security of that information.

Employees are only to use smart phones supplied and supported by Information Services. Access to the device is to be restricted by a unique password created by the device owner. Passwords are not to be divulged to a third party and the device is to be secured at all times. Employees are to report loss, damage or compromise of the PSD to their manager and Information Services as soon as it is suspected or discovered.

The Chief Information Officer is responsible for implementing policy and procedures on use of PSD.

The Director of Property will ensure that the device memory will be cleared on disposal of the PSD.

6.2.7 Facsimiles, Scanners and Photocopiers

Care is to be taken when photocopying personal information on multi-function machines containing facsimiles or scanners not to deliberately or inadvertently transmit personal information to third parties not authorised to receive it.

6.2.8 Weekly back up

Information Services is responsible for the back-up of information stored our electronic data systems to insure the integrity of data.

6.2.9 Clear desk policy

Employees are to make reasonable efforts to secure or conceal personal information when away from their work space, after hours or when their office is attended by people not authorised to view it.

6.2.10 After hours access

Access to office facilities is granted only to people with a business need.

6.2.11 Carriage of documents outside the office

Documents displaying personal information, such as client files, are to be covered when carrying files outside the office.

This policy also applies to files transferred between floors at 444 Queen Street, Brisbane, and other sites we share with third parties.

6.2.12 Movement of documents between offices

When moving personal information by mail between offices, employees are to use the services of the approved courier service. The Records Management team can advise employees of the approved secure courier services we use.

6.2.13 Discussion of personal information

Employees are not to discuss personal information with unauthorised officers and non-employees. Employees must be take caution when holding discussions with others in public spaces/ reception areas.

Employees should not discuss personal information outside work premises. This includes veiled references to individuals. If for operational reasons discussions have to take place away from the office then employees must ensure they are not overheard.

6.2.14 Loss, unauthorised disclosure and security breaches

If personal information is lost or compromised we will consider the context of the personal information and circumstances of the breach before deciding to notify the people affected by the event.

6.3 IPP 5 – 7: Providing information, access and amendment

Where we have control of documents containing personal information, all reasonable steps are taken to ensure that a person can find out:

- the types of personal information we hold;
- the main purposes for which the personal information is used; and
- what steps they need to take to obtain access to their personal information.

Members of the public and employees are entitled to request access to any record containing their personal information and request amendments if those records are inaccurate.

6.3.1 Access applications

Under the IP Act there are controls on how personal information is managed. The rights of access and amendment are dealt with in IPP 6 and 7. Those rights are confined to the person to whom the personal information directly and personally relates.

In addition, section 14 of the *Public Service Regulation 2008* provides that a public sector employee can request to inspect or take an extract from their own employee record held by the department.

There are two ways of accessing personal information which are set out below.

6.3.2 Administrative Access & Release

Administrative access schemes are designed to give individuals access to their own personal information or to non-sensitive information, except where legislation (e.g. *Adoption Act 2009* (QLD) prevents such release or the information contains personal information of another person. It is discretionary, and does not have the rights of review available to applicants under statutory access schemes. Administrative release allows us to give access to certain types of information as a matter of course without the need for a formal application under legislative schemes such as the RTI and IP Acts.

Wherever possible personal information is to be released administratively unless there is a legislative, policy or administrative reason restricting or preventing access (refer to IPP 6). Refer to our Administrative Release Policy for more information.

6.3.3 Information Privacy (IP) access application

Where information cannot be administratively released, the person will be asked to submit a written application following the process detailed on our website at http://www.pt.qld.gov.au/right-to-information/index.html. There is no application fee for IP Access Applications which should be sent to:

Governance and Executive Directorate
The Public Trustee of Queensland
GPO Box 1449
Brisbane QLD 4001

Before lodging an access application the applicant may want to contact the Governance and Executive Directorate on (07) 3213 9172 or email at governance@pt.qld.gov.au.

6.4 Amendment

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

Applications to amend personal information must be in writing with particulars of the information to be amended. A *Privacy Application Amendment From* is available from the Queensland Government website http://www.rti.qld.gov.au/__data/assets/pdf_file/0009/97335/attachment-4-approved-form-2ip_s.FH11.PDF. Download and complete the form and send it to Governance and Executive Directorate at the above address.

6.5 IPP 8 – 9: Accuracy and relevance of personal information

All reasonable precautions will be taken to ensure that personal information is accurate, complete and up-to-date before it is used. The accuracy of that information depends largely on the information received. Therefore, members of the public and employees are encouraged to:

- inform us if there are known errors in their personal information; and
- keep us advised of changes to personal information.

6.5.1 Accuracy of information

Before employees use personal information to make decisions on behalf of, or provide services to individuals (clients, employees and members of the public) they must take reasonable steps to check the currency, accuracy and completeness of the personal information.

Each program will implement and maintain procedures to ensure that decisions made about individuals are based on accurate, complete and up-to-date information.

6.5.2 Relevant purpose

Employees are to ensure that personal information is only used for a particular purpose directly related to our activities. In addition employees must only use those parts of the personal information directly relevant to fulfilling the particular purpose for which the information was collected.

6.6 IPP 10 – 11: Use and disclosure of personal information

6.6.1 Use for appropriate purpose

Employees are not to collect or use personal information for personal gain, or purposes not directly related to business activities. Employees must only access personal information (including client or employee files) only where it is a direct requirement of their role.

We may use personal information if the:

- individual has expressly or impliedly agreed to the use for the secondary purpose.
- secondary purpose is directly related to the primary purpose.
- use is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare.
- use is authorised or required under law.
- use is necessary for certain types of law enforcement purposes.
- use is necessary for certain types of research, or the compilation or analysis of statistics, in the public interest; the use does not involve the publication of all or any of the personal information in a form that identifies any particular individual the subject of the personal information; and it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.

6.6.2 Disclosure

Where we possess or control a document containing personal information collected for a particular purpose then, we must not disclose that information for another purpose unless:

- the person concerned has expressly or impliedly agreed to disclosure of the information for the other purpose.
- Public Trustee is satisfied on reasonable grounds that the use of the information is necessary to lessen or prevent serious threat to the life, health, safety or welfare of an individual or to public health, safety or welfare.
- Public Trustee is authorised by law to do so.
- it is necessary for certain types of law enforcement.
- the information is necessary for certain types of research, or the compilation or analysis of statistics in the public interest; and does not involve the publication of personal information; it is not practicable to obtain the express or implied agreement of the individual before the disclosure; and we are satisfied the relevant entity will not disclose the personal information to another entity.

- the other purpose is directly related to the purpose for which the information was obtained.

Where a disclosure occurs under one of these exceptions, we must take reasonable steps to ensure that the third party does not use or disclose the information for a purpose other than the purpose for which it was disclosed.

For example, there is a requirement to include a record of the use where personal information is used for law enforcement purposes.

7. Documents to which the privacy principles do not apply

Schedule 1 of the IP Act details the documents to which the privacy principles do not apply.

8. Privacy complaints

If an individual believes that we have not dealt with their personal information in accordance with the IP Act they may make a privacy complaint. Privacy complaints should be put in writing with as much detail as possible. The complaint should be marked 'Private and Confidential' and sent to:

Director
Governance & Executive Directorate
The Public Trustee of Queensland
GPO Box 1449
Brisbane QLD 4001

Email governance@pt.qld.gov.au
Phone: 07 3213 9160 **Fax:** 07 3213 9489

Written complaints will be acknowledged in writing within three working days from receipt. The IP Act allows agencies 45 business days to resolve privacy complaints. Complaints will be processed in accordance with our Information Privacy Complaints Management Policy and Procedure.

9. Complaints to Office of the Information Commissioner

If a complainant is not satisfied with our response or does not receive one within 45 business days, then they may refer a written complaint to the Office of the Information Commissioner (OIC).

The OIC is an independent statutory authority empowered under the IP Act to mediate and resolve privacy complaints where the complainant has previously lodged a complaint with a government agency, but remains dissatisfied with the outcome of that process.

Complaints to the OIC must be made in writing either by completing a hard copy of the complaint form contained on the website http://www.oic.qld.gov.au/about/privacy/privacy-complaints , lodging it online, or by letter, and either hand delivering, posting, faxing or emailing it to the OIC office at:

Postal address
Office of the Information Commissioner
PO Box 10143, Adelaide St
Brisbane QLD 4000
email: administration@oic.qld.gov.au

Office address
Level 8, 160 Mary Street
BRISBANE QLD 4000

Telephone: 07 3405 1111
Fax: 07 3405 1122

If the complaint is unable to be mediated by the OIC then the complainant can require the OIC to refer its complaint to the Queensland Civil and Administrative Tribunal for a hearing.

10. Legislation requiring the collection of personal information

We collect personal information under a number of Acts. A full list of the types of information collected and the covering Acts are listed in our Privacy Information Digest.