The Public Trustee

Information Privacy Plan

February 2019

Document Information

Approved

Name	Position	Signature	Date
Peter Carne	The Public Trustee of Queensland		

Endorsed

Name	Approval	Date
Josephine Giles	Senior Director Governance and Risk	22.12.19
Executive Management Team	Version 6.0 endorsed at meeting	04.12.18

Revision History

Version	Date	Revised By	Change
0.1	28 Oct 2011	RTI, Privacy & Project Management Officer	Created first version
0.1.2	14 Nov 2011	RTI, Privacy & Project Management Officer	First draft circulated for feedback
1.0	4 Jan 2012	RTI, Privacy & Project Management Officer	Final for approval
2.0	17 Dec 2012	Governance Officer	Incorporate review changes
3.0	7 Jan 2013	Principal Governance Officer	Incorporate review changes
4.0	June 2014	Governance Officer	Incorporate review changes
5.0	August 2014	Governance Officer	Incorporate OIC suggestions
6.0	November 2018	Privacy Officer	Review in response to the recommendations of an Internal Audit of Information Privacy
6.1	February 2019	Privacy Officer	Furthr amendments to incorporate feedback from Manager, Security and Business Resilience

Contact

Policy Owner:	Governance and Risk Directorate
Contact Details:	governance@pt.qld.gov.au
Document Status:	Review
File:	G:\Governance & Risk Directorate\GRD Internal Audit Reports

Contents

1. Introduction

The *Information Privacy Act 2009* (Qld) (IP Act) commenced on 1 July 2009. The IP Act regulates how Queensland public sector agencies including the Public Trustee, manage the collection, storage, use and disclosure of personal information. The IP Act:

- creates an obligation to comply with eleven Information Privacy Principles (IPPs);
- regulates when personal information may be transferred outside of Australia; and
- outlines the obligations regarding contracted service providers.

2. Compliance with the Information Privacy Principles

The IPPs set out the Public Trustee's obligations regarding how personal information must be managed. The IPPs deal with the following:

IPP 1: Collection of personal information (lawful and fair)
IPP 2: Collection of personal information (requested from individual)
IPP 3: Collection of personal information (relevance)
IPP 4: Storage and security of personal information
IPP 5: Providing information about documents containing personal information
IPP 6: Access to documents containing personal information
IPP 7: Amendment of documents containing personal information
IPP 8: Checking of accuracy of personal information before use by agency
IPP 9: Use of personal information only for relevant purposes
IPP 10: Limits on use of personal information
IPP 11: Limits on disclosure

IPP 5 places an obligation on the Public Trustee to take steps to ensure that individuals are aware of the types of personal information held by the agency, the purpose for which it is held, and how an individual can request access to their own personal information. This document is designed to meet the Public Trustee's obligations under IPP5 to take reasonable steps to ensure that individuals can find out:

- if the Public Trustee controls any documents containing personal information;
- the type of personal information in those documents;
- the main purposes for which that personal information is collected, held and used; and
- how an individual can access and amend their own personal information held by the Public Trustee.

The aim of this Information Privacy Plan is to assist employees, clients and members of the public to understand how the Public Trustee manages personal information in accordance with the IP Act.

3. What is personal information?

Personal information is defined in section 12 of the IP Act 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 may be stored in a variety of media including paper, an electronic database, correspondence, photographic or video images, digital format and audio recordings.

Personal information, as defined in the IP Act, does not apply to information in generally available publications or sources such as newspapers, magazines, journals, books, legislation and regulations etc.

4. About the Public Trustee

The Public Trustee of Queensland (the Public Trustee) operates as a corporation sole and has been serving Queenslanders since 1916. The Public Trustee is governed by the *Public Trustee Act 1978*.The Public Trustee provides financial, trustee and legal services to the people of Queensland. These services are delivered through a network of regional offices, outreach locations and supported by the Queensland Government Agent Program.

The Public Trustee's vision is to be the independent trustee for Queenslanders providing security and peace of mind. Our services include:

- Acting as Financial Administrator for adults with impaired capacity for decision making
- Preparing Wills and Enduring Powers of Attorney (EPAs).
- Administering Deceased Estates.
- Acting as Financial Attorney under EPAs.
- Acting as Trustee for Minors, Charitable and other Trusts
- Administering Unclaimed Moneys for the State of Queensland
- Acting as manager of the estate of prisoners liable to imprisonment for 3 years or more.
- Criminal confiscation matters - collecting, managing and selling property, chattels and goods restrained or forfeited under the *Criminal Proceeds Confiscation Act 2002* when ordered by the Court to do so.

5. What types of personal information are collected and held by the Public Trustee?

In delivering services to the people of Queensland the Public Trustee collects 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 Public Trustee collects and manages a wide range of personal information about individuals as part of performing its functions, from:

- clients and their family members;
- employees, including prospective employees, and contractors;
- non-government service providers;
- local and state and federal government agencies;
- vendors and service providers.

The Public Trustee collects and manages personal information about individual clients of the Public Trustee including the following information as a minimum:

- full name (including maiden names, birth/adopted names, aliases);
- address (residential and postal);
- phone number (landline and mobile);
- email address;
- date of birth (or age);
- place of birth;
- marital status;
- gender;
- spouse/parents/children/next of kin details; and
- occupation.

Further personal information collected depends upon the services provided and may include:

- copies of official documents (Driver's Licence, Passport, Citizenship papers, Birth Certificate);
- Tax File Number (TFN);
- property addresses and details of other investments;
- financial institution account details;
- reference numbers (our identification numbers or those of other organisations);

- details of income, assets and liabilities;
- employment history or details;
- signature;
- photographs of individuals (in some cases);
- relationship details and family circumstances;
- family history;
- medical/health/diagnostic information;
- service provision needs;
- occupation and employment history; and
- details of office bearers in funded organisations (i.e. names)

Certain functions and work groups may also require collection of additional information as required to fulfil their role.

The Public Trustee may also collect personal information in undertaking its regulatory, legislative and administrative activities:

- personal information of persons making complaints, subjects of complaints, and personal information related to complaint investigations.
- recruitment information e.g. applications for employment with the Public Trustee, records relating to referee checks, interview notes and selection panel assessments etc.
- personal information of staff members that is received or collected in the course of conducting human resource management functions (e.g. leave entitlements, bank account details, superannuation information, pay scale)
- personal information recorded by way of camera surveillance systems or electronic monitoring devices in Public Trustee premises and public contact areas.

When collecting personal information, the Public Trustee takes reasonable steps to explain why personal information is collected, what is done with it, whether any law requires its collection and identifies other entities to which it may be disclosed. This explanation may be provided in writing or given verbally.

6. Storage and management of personal information

The personal information we collect is generally stored in electronic databases including, but not limited to, a client information database, Human Resources system, accounting software and others as required by internal workgroups.

Information is also stored on desktop computers, laptops, external hard drives, mobile devices and work group directories allocated by the Information Systems work group.

Hardcopies of information are stored in secure locations. We take reasonable precautions to protect personal information against loss, unauthorised access, use, modification, disclosure or other forms of misuse.

The Public Trustee is required to comply with the Queensland Government's Records Governance Policy and the *Public Records Act 2002* which ensure that the records of Queensland Government agencies are complete, reliable and accessible and if appropriate, retained in a usable form for the benefit of present and future generations.

7. What does the Public Trustee do with personal information?

The Public Trustee collects personal information to perform its functions and to undertake its administrative and statutory responsibilities. The Public Trustee will use and disclose the information only as necessary for that purpose: for example, to administer the financial affairs of adults with impaired capacity for decision making when the Public Trustee is appointed as financial administrator

Sometimes the Public Trustee may use or disclose personal information for a purpose other than that for which it was collected if, for example:

- where the information will be used for a purpose that is *directly related* to the purpose for which it was collected, for instance making contact with a beneficiary of a Will where the Public Trustee is appointed as the executor and is managing the estate of the deceased.
- where the person from whom the personal information was collected is *reasonably likely to have been aware* under IPP2 that it is our usual practice to disclose that type of information to a particular person or entity (for example, when acting on behalf of the client as the Financial Attorney under an Enduring Power of Attorney).
- where the person has *expressly or impliedly consented* to the proposed use or disclosure.
- where we are satisfied on reasonable grounds that the use or disclosure is necessary to lessen or prevent a *serious threat to the life, health, safety or welfare* of an individual or the public (for example, providing information to the police about a missing person to help to locate the person).
- where the use or disclosure is *authorised or required by law* (for example, in response to a subpoena from a Court).
- where we are satisfied on reasonable grounds that the use or disclosure is necessary for *law enforcement* processes (for example, in the investigation by police of a criminal offence).
- where the use or disclosure is for *research* in the public interest and certain requirements are met.
- For marketing purposes where the use is in accordance with the IPP 11(4) and the individual is given the opportunity to opt out.

8. Contracted service providers and personal information

Sections 34 - 37 of the IP Act regulate how personal information is managed when the Public Trustee enters into a contract or other arrangement for the provision of services associated with the performance of any of the Public Trustee's functions, where the services involve dealing with personal information.

In particular, the Public Trustee must take all reasonable steps to bind the service provider to comply with the relevant Privacy Principles in the IP Act in discharging its obligations under the service arrangement. If the Public Trustee does not take such reasonable steps to bind the service provider to comply with the Privacy Principles, the contractual obligations will attach to the Public Trustee.

9. Transferring personal information outside of Australia

The IP Act also regulates the transfer of personal information to entities outside of Australia. This issue is relevant in the context of personal information of clients, service providers, staff and other persons involved with the Public Trustee being transmitted or held on computer networks and servers outside Australia. The IP Act allows the transfer of personal information outside of Australia only in certain circumstances, such as:

- when the individual has agreed;
- the transfer is authorised or required under a law;
- the agency is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of any individual, or to public health, safety and welfare; or
- if two or more of the following criteria apply:
  - the recipient is subject to equivalent privacy obligations;
  - the transfer is necessary to perform a function of the department;
  - the transfer is for your benefit;
  - reasonable steps have been taken by the agency to ensure the information is protected.

An example of where the Public Trustee may transfer personal information outside of Australia includes where a member of the public has requested we correspond with them using a web based email service whose servers are based in another country.

10. Access to personal information held by the Public Trustee

The rights of access and amendment are dealt with in IPP 6 and 7 of the IP Act and are available to an individual to whom the personal information directly relates.

The Public Trustee's administrative access scheme allows for the Public Trustee to provide access to a range of documents and information to an individual about themselves as a matter of course without the need for a formal application under legislative schemes such as the IP Act. Please refer to the Public Trustee's Administrative Access Policy and Procedure.

If the applicant is dissatisfied with the response to their administrative request for their personal information, they maintain the right to apply for access to the information under the IP Act.

Please note, as part of the access application process, we will ask you to provide us with proof of identity and make your request in writing as follows.

Access applications under the IP Act are processed by the Department of Justice and Attorney-General (DJAG). These applications can be completed online by selecting DJAG as the agency. You can also download the Right to Information and Information Privacy Access Application Form and the Personal Information Amendment Form. For more information about the Right to Information and Information Privacy process, visit the Office of the Information Commissioner website.

Under the RTI and IP Acts, you have a right of internal review. An internal review decision must not be decided by the person who made the original decision, or a person who is less senior than that person. An application for internal review must be made in writing, state an address to which notices under the relevant Act may be sent, and be lodged at the following address:

RTI and Privacy Unit
Department of Justice and Attorney-General
GPO Box 149
Brisbane Qld 4001
Telephone: (07) 3227 7618
Email: rtiadministration@justice.qld.gov.au

There is no fee for internal review applications. Unless a further time is allowed, an application for internal review must be made within 20 business days after the date of the written notice of the decision.

You may also apply to have any decision externally reviewed by the office of the Information Commissioner. It is not necessary to have an internal review before applying for external review. An application for external review can be lodged with the Office of the Information Commissioner. See their website for further information.

In addition, current employees of the Public Trustee can, under section 14 of the *Public Service Regulation 2008*, request to inspect or copy an extract from their own employee record held by the Public Trustee.

11. Information Privacy (IP) access application

Where information cannot be administratively released, an individual can submit a written application following the process detailed at the Queensland Government Right to Information website at www.rti.qld.gov.au. There is no application fee for an individual to access their own personal information under the IP Act.

12. Amendment of personal information

If an individual considers that the personal information the Public Trustee holds about them is incorrect, misleading, incomplete or out of date, they may seek to amend the personal information under the IP Act by submitting a written application following the process detailed at the Queensland Government Right to Information website at www.rti.qld.gov.au.

Before lodging an amendment application the applicant may want to contact the Public Trustee's Privacy Officer on (07) 3564 2103 or email at governance@pt.qld.gov.au to discuss their concerns.

13. Privacy complaints

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

Senior Director
Governance and Risk Directorate
The Public Trustee of Queensland
GPO Box 1449
Brisbane QLD 4001
Email: governance@pt.qld.gov.au

Individuals may also contact the Public Trustee's Privacy Officer to discuss their concerns on 07 3564 2103.

Complaints will be acknowledged in writing within five working days from receipt. The IP Act allows agencies 45 business days to resolve privacy complaints. Privacy complaints will be dealt with in accordance with the Public Trustee's Information Privacy Complaints Management Policy and Procedure.

14. Office of the Information Commissioner

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 Queensland Government agency, but remains dissatisfied with the outcome of that process.

If a complainant is not satisfied with the response from the Public Trustee or does not receive a response within 45 business days, they may make a complaint to the Office of the Information Commissioner (OIC) Queensland.

Information about making a complaint to the Office of the Information Commissioner may be accessed by visiting their website at: www.oic.qld.gov.au

15. Appendix 1 – Information Privacy Principles

Information Privacy Act 2009 – Schedule 3 - Information Privacy Principles

IPP 1 – Collection of personal information (lawful and fair)

(1) An agency must not collect personal information for inclusion in a document or generally available publication unless –

(a) the information is collected for a lawful purpose directly related to a function or activity of the agency; and

(b) the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.

(2) An agency must not collect personal information in a way that is unfair or unlawful.

IPP 2 – Collection of personal information (requested from individual)

(1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

(2) However, this section applies only if the agency asks the individual the subject of the personal information for either –

(a) the personal information; or

(b) information of a type that would include the personal information.

(3) The agency must take all reasonable steps to ensure that the individual is generally aware of –

(a) the purpose of the collection; and

(b) if the collection of the personal information is authorised or required under a law –

(i) the fact that the collection of the information is authorised or required under a law; and

(ii) the law authorising or requiring the collection; and

(c) if it is the agency's usual practice to disclose personal information of the type collected to any entity (the ***first entity***) – the identity of the first entity; and

(d) if the agency is aware that it is the usual practice of the first entity to pass on information of the type collected to another entity (the ***second entity***) – the identity of the second entity.

(4) The agency must take the reasonable steps required under subsection (3) –

(a) if practicable – before the personal information is collected; or

(b) otherwise – as soon as practicable after the personal information is collected.

(5) However, the agency is not required to act under subsection (3) if the personal information is collected in the context of the delivery of an emergency service; and

Example –

personal information collected during a triple 0 emergency call or during the giving of treatment or assistance to a person in need of an emergency service

IPP 3 – Collection of personal information (relevance etc.)

(1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

(2) However, this section applies to personal information only if the agency asks for the personal information from any person.

(3) The agency must take all reasonable steps to ensure that –

(a) the personal information collected is –

(i) relevant to the purpose for which it is collected; and

(ii) complete and up to date; and

(b) the extent to which personal information is collected from the individual the subject of it, and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.

IPP 4 – Storage and security of personal information

(1) An agency having control of a document containing personal information must ensure that –

(a) the document is protected against –

(i) loss; and

(ii) unauthorised access, use, modification or disclosure; and

(iii) any other misuse; and

(b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.

(2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

IPP 5 – Providing information about documents containing personal information

(1) An agency having control of documents containing personal information must take all reasonable steps to ensure that a person can find out –

(a) whether the agency has control of any documents containing personal information; and

(b) the type of personal information contained in the documents; and

(c) the main purposes for which personal information included in the documents is used; and

(d) what an individual should do to obtain access to a document containing personal information about the individual.

(2) An agency is not required to give a person information under subsection (1) if, under an access law, the agency is authorised or required to refuse to give that information to the person.

IPP 6 – Access to documents containing personal information

(1) An agency having control of a document containing personal information must give an individual the subject of the personal information access to the document if the individual asks for access.

(2) An agency is not required to give an individual access to a document under subsection (1) if –

(a) the agency is authorised or required under an access law to refuse to give the access to the individual; or

(b) the document is expressly excluded from the operation of an access law.

IPP 7 – Amendment of documents containing personal information

(1) An agency having control of a document containing personal information must take all reasonable steps, including by the making of an appropriate amendment, to ensure the personal information –

(a) is accurate; and

(b) having regard to the purpose for which it was collected or is to be used and to any purpose directly related to fulfilling the purpose, is relevant, complete, up to date and not misleading.

(2) Subsection (1) applies subject to any limitation in a law of the State providing for the amendment of personal information held by the agency.

(3) Subsection (4) applies if –

(a) an agency considers it is not required to amend personal information included in a document under the agency's control in a way asked for by the individual the subject of the personal information; and

(b) no decision or recommendation to the effect that the document should be amended wholly or partly in the way asked for has been made under a law mentioned in subsection (2).

(4) The agency must, if the individual asks, take all reasonable steps to attach to the document any statement provided by the individual of the amendment asked for.

IPP 8 – Checking of accuracy etc. of personal information before use by agency

Before an agency uses personal information contained in a document under its control, the agency must take all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, complete and up to date.

IPP 9 – Use of personal information only for relevant purpose

(1) This section applies if an agency having control of a document containing personal information proposes to use the information for a particular purpose.

(2) The agency must use only the parts of the personal information that are directly relevant to fulfilling the particular purpose.

IPP 10 – Limits on use of personal information

(1) An agency having control of a document containing personal information that was obtained for a particular purpose must not use the information for another purpose unless –

(a) the individual the subject of the personal information has expressly or impliedly agreed to the use of the information for the other purpose; or

(b) the agency is satisfied on reasonable grounds that use of the information for the other purpose 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; or

(c) use of the information for the other purpose is authorised or required under a law; or

(d) the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary for 1 or more of the following by or for a law enforcement agency –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court of tribunal; or

(e) the other purpose is directly related to the purpose for which the information was obtained; or

Examples for paragraph (e) –

1. An agency collects personal information for staff administration purposes. A new system of staff administration is introduced into the agency, with much greater functionality. Under this paragraph, it would be appropriate to transfer the personal information into the new system.
2. An agency uses personal information, obtained for the purposes of operating core services, for the purposes of planning and delivering improvements to the core services.

(f) all of the following apply –

(i) the use is necessary for research, or the compilation or analysis of statistics, in the public interest;

(ii) 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;

(iii) it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.

(2) If the agency uses the personal information under subsection (1)(d), the agency must include with the document a note of the use.

IPP 11 – Limits on disclosure

(1) An agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the ***relevant entity***), other than the individual the subject of the personal information, unless –

(a) the individual is reasonably likely to have been aware, or to have been made aware, under IPP 2 or under a policy or other arrangement in operation before the commencement of this schedule, that it is the agency's usual practice to disclose that type of personal information to the relevant entity; or

(b) the individual has expressly or impliedly agreed to the disclosure; or

(c) the agency is satisfied on reasonable grounds that the disclosure is necessary to lessen or prevent a

serious threat to life, health, safety or welfare of an individual, or to public health, safety or welfare; or

(d) the disclosure is authorised or required under a law; or

(e) the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for 1 or more of the following by or for a law enforcement agency –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court of tribunal; or

(ea) all of the following apply—

(i) ASIO has asked the agency to disclose the personal information;

(ii) an officer or employee of ASIO authorised in writing by the director-general of ASIO for this paragraph has certified in writing that the personal information is required in connection with the performance by ASIO of its functions;

(iii) the disclosure is made to an officer or employee of ASIO authorised in writing by the director-general of ASIO to receive the personal information; or

(f) all of the following apply –

(i) the disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;

(ii) the disclosure does not involve the publication of all or any of the personal information in a form that identifies the individual;

(iii) it is not practicable to obtain the express or implied agreement of the individual before the disclosure;

(iv) the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.

(2) If the agency discloses the personal information under subsection (1)(e), the agency must include with the document a note of the disclosure.

(3) If the agency discloses personal information under subsection (1), it must take all reasonable steps to ensure that the relevant entity will not use or disclose the information for a purpose other than the purpose for which the information was disclosed to the agency.

(4) The agency may disclose the personal information under subsection (1) if the information may be used for a commercial purpose involving the relevant entity's marketing of anything to the individual only if, without limiting subsection (3), the agency is satisfied on reasonable grounds that –

(a) it is impracticable for the relevant entity to seek the consent of the individual before the personal information is used for the purposes of the marketing; and

(b) the relevant entity will not charge the individual for giving effect to a request from the individual to the entity that the individual not receive any marketing communications; and

(c) the individual has not made a request mentioned in paragraph (b); and

(d) in each marketing communication with the individual, the relevant entity will draw to the individual's attention, or prominently display a notice, that the individual may ask not to receive any further marketing communications; and

(e) each written marketing communication from the relevant entity to the individual, up to and including the communication that involves the use, will state the relevant entity's business address and telephone number and, if the communication with the individual is made by fax, or other electronic means, a number or address at which the relevant entity can be contacted electronically.