INFORMATION PRIVACY ACT 2009
OBLIGATIONS OF CONTRACTED SERVICE PROVIDERS

Background and purpose

The Department of Communities, Disability Services and Seniors (**the department**) engages service providers to assist with its functions. For the purposes of the *Information Privacy Act 2009* (**IP Act**), these entities are described as 'contracted service providers' (**CSPs**).

In the course of fulfilling contracts, CSPs often handle personal information of individuals. The standard terms of the department's contracts require CSPs to comply with relevant provisions of the IP Act in relation to that personal information.

Where a CSP is required to comply with the IP Act, the CSP is defined as a 'bound contracted service provider'.

If a bound CSP fails to comply with the standard terms, not only will the CSP be in breach of the contract, but will be liable under the IP Act for any breach of privacy that it commits (sections 34-37 of the IP Act).

The purpose of this fact sheet is to indicate the nature of the obligations of a bound CSP. However, it does not include specific guidance as to how a bound CSP should perform its obligations because compliance is a matter for each CSP. Given the statutory liability that falls on CSPs under the IP Act, the department is not able to provide specific advice to a CSP on its privacy obligations.

Guidance on the operation of the IP Act is published on the Queensland Office of the Information Commissioner (**OIC**) website at http://www.oic.qld.gov.au. Additional privacy information is available on the Office of the Australian Information Commissioner website https://www.oaic.gov.au/.

However, if a CSP is unsure as to its obligations, the CSP should obtain independent legal advice.

The overview below is intended only to alert CSPs who are unfamiliar with the IP Act, to likely issues. The department assumes that each CSP will develop its own full privacy policy and procedures with reference to the IP Act.

Obligations under *Information Privacy Act 2009*

The IP Act requires a bound CSP to comply with the 11 Information Privacy Principles (**IPPs**) set out in schedule 3 of the Act[1].

Additionally, a bound CSP is required to comply with section 33 of the IP Act, which prohibits the transfer of personal information outside Australia, except in limited circumstances. CSPs should note that an example of when personal information may be transferred outside Australia is if it uses a cloud based service provider which is located

[1] *If the CSP is a 'health agency' [as defined in the IP Act], the CSP will be obliged alternatively to comply with the National Privacy Principles (NPPs) set out in schedule 4 of the Act. However, this department does not normally engage CSPs as health agencies. In the circumstances, this fact sheet does not discuss the NPPs.*

overseas. The terms of the standards contract require CSPs to obtain the department's consent to any proposed overseas transfer of personal information. Generally, the department will not consent to sensitive personal information being sent overseas.

If a person alleges that a bound CSP has breached an IPP or section 33 in relation to their personal information, it is the CSP's responsibility to deal with the complaint.

If the complainant is dissatisfied with the CSP's response, they may take the complaint to the OIC. The OIC will attempt to resolve the matter by mediation. If that process fails, the matter may be referred to the Queensland Civil and Administrative Tribunal (**QCAT**) for decision.

If QCAT finds that they complaint, or a part of the complaint, has been substantiated, it may make a variety of orders, including an award of compensation against the CSP of up to $100,000 per breach.

Other obligations under standard terms of contract
The standard terms of the department's contracts also require the CSP to notify the department of any breach of the privacy requirements under the IP Act or contract.

A breach of privacy may involve the privacy of a single individual. However, a general loss of data may occur. For example, the CSP's computer system could be hacked, or a laptop could be stolen. In any event, the department will want to ensure any potential harm is avoided or minimised. For this reason, the department must be notified as soon as possible about any privacy breaches.

Notification of a breach does not mean that the CSP is absolved of responsibility for taking its own remedial action.

Obligations under other legislation
The IP Act is subject to other legislation that may specifically restrict the disclosure of information, such as the confidentiality provisions in the *Child Protection Act 1999*. The department expects each CSP to be aware of any legislation relevant to the performance of its contractual obligations.

A CSP may in its own right be subject to the Commonwealth *Privacy Act 1988*. However, that Act does not override the CSP's obligations to comply with the Queensland IP Act nor the terms of any State contract (see sections 3 and 7B of the *Privacy Act 1988*).

'Personal information'
The IPPs (summarised below) govern the collection, management, use and disclosure of all personal information.

As a fundamental requirement, CSP staff should be able to recognise what constitutes personal information.

'Personal information' is defined in section 12 of the IP Act:

> *Personal information is 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.*

'Individual' means a natural person as opposed to, for example, a company or corporation.

A comprehensive list of personal information may be found in the department's Privacy guide but includes:

- name, date and place of birth
- race or ethnicity
- financial/banking details
- health/diagnostic information
- employment details
- photograph (including images captured on CCTV)
- signature
- uniquely identifying number – e.g. driver license number, tax file number, employee number
- details of services requested or obtained by a person
- unique physical characteristics – e.g. tattoo, birthmark

Personal information may reveal a person's identity even if their name is not mentioned. Other information may enable their identity to be deduced.

A CSP's privacy obligations remain as long as it has possession of or control over the personal information.

Whenever a CSP staff member proposes to collect or deal with personal information in any way, they must consider whether what they propose is in accordance with the IP Act.

The Information Privacy Principles

The IPPs set out how personal information is to be collected, handled and accessed. The IP Act should be consulted for the full requirements, but provided below is a summary of the 11 IPPs:

IPP 1 – Collection of personal information must be lawful, fair, and necessary for the agency's functions.

IPP 2 – Where an agency requests an individual to provide personal information, the agency must advise the individual of the purpose of the collection, any laws which give the agency authority to collect the information, and to whom the agency usually discloses or gives the information.

> *NOTE: The advice required by IPP2 may be given orally or in writing. If the collection is in writing, a written notice is usually more appropriate.*

IPP3 – Personal information that is collected must be relevant, up-to-date and complete. The collection must not be an unreasonable intrusion into the personal affairs of the individual.

IPP 4 – The agency must ensure personal information is protected against loss, unauthorised access or other misuse. The safeguards must be *'adequate to provide the level of protections that can reasonably be expected to be provided'*.

CSPs should have procedures that deal with:

• physical security (e.g. access to premises; clean desk policy; rules about removal of files and mobile devices from the office; conducting interviews in private); and
• digital security (e.g. up to date access permissions; use of complex passwords; software updates; regular audits).

IPP 5 – The agency must ensure individuals can find out what personal information is held about themselves.

IPP 6 – The agency must give the individual access to their personal information unless a law allows for refusal[2].

IPP 7 – An individual has the right to require correction or amendment of their personal information, or alternatively the agency must attach a statement of correction.

IPP 8 – Before using personal information, an agency must take reasonable steps to check the information is accurate, complete and up to date.

IPP 9 – An agency must only use personal information for its original intended purpose.

IPP10 – An agency may only use[3] personal information for its original intended purpose, subject to the listed exceptions.

IPP11 – An agency may only disclose[3] personal information in the listed circumstances.

Policy and practice
The department would suggest that each CSP develops specific privacy policy and procedures to assist staff with reference to the categories of personal information that they handle.

Additionally, each CSP may find it useful to train a specific staff member to deal with privacy related issues.

Resources
Information Privacy Act 2009 (Qld)
Office of the Information Commissioner (Qld)

[2] For example, the IP Act provides for information that is exempt from disclosure or contrary to public interest and grounds for refusal. (refer to Chapter 3 of the IP Act, and the *Right to Information Act 2009*, schedules 1-4.)
[3] Section 23 of the IP Act defines 'use' and 'disclosure' for purposes of IPPs 10 and 11.