Contracted service providers and the Queensland Privacy Principles (QPPs)

Background

The Department of Families, Seniors, Disability Services and Child Safety (**the department**) engages contracted service providers (**CSPs**) to perform some of its functions.

CSPs often handle personal information while performing those functions. The department wants to ensure that personal information is protected, whether it is being handled by departmental or CSP employees.

The standard terms of Queensland Government contracts bind CSPs to comply with **chapter 2, parts 1 and 2 and section 41** of the *Information Privacy Act 2009* (**IP Act**) in relation to personal information.[1]

Information privacy is also covered by the Human Services Quality Framework for CSPs providing human services (standard 1.7).

Note: This fact sheet only applies to CSPs which are contractually bound to comply with **chapter 2, parts 1 and 2, and section 41** of the IP Act.

Personal information

The IP Act governs collection, management, use and disclosure of personal information.

Personal information is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable from the information or opinion, whether it is true or not, and whether it is recorded in a material form or not. (s12 IP Act)

An *individual* is a natural person and does not include a company or corporation.

Information may reveal a person's identity even if their name is not mentioned, if their identity can be deduced.

CSP staff must be able to identify personal information and how it should be managed.

'Sensitive information'

IPOLA also introduces the concept of sensitive information, which includes personal information such as racial or ethnic origin, religious belief and affiliations, sexual orientation and practices, criminal history, medical, genetic and biometric information.

QPPs 3 and 6 contain rules about collection, use and disclosure of sensitive information.

Obligations under the IP Act

If a CSP has been bound to comply with chapter 2, parts 1 and 2, and section 41 of the IP Act, they must comply with the Queensland Privacy Principles (**QPPs**), section 33 (overseas disclosure) and any QPP codes approved by regulation.

Privacy policy

QPP1 requires that bound CSPs have a privacy policy that outlines how they protect the privacy of people whose personal information they handle.

The Office of the Australian Information Commissioner has guidelines about developing a privacy policy on its website.

Privacy practice

CSPs must provide regular (e.g. annual) privacy training to all staff, to ensure that they understand their privacy obligations.

[1] These obligations came into effect on 1 July 2025. CSPs which contracted with Queensland Government before that date and have not varied the terms of their contract may have different privacy obligations. If so, you should refer to the *Contracted service providers and the IPPs fact sheet.*

CSPs may also find it useful to nominate a staff member to be a Privacy Contact Officer, to provide privacy guidance and advice to other staff and deal with privacy issues.

If a bound CSP fails to comply with its privacy obligations, it will be liable for any breaches under the IP Act (including potential liability to pay compensation of up to $100,000 per breach) and possibly breach of contract.

Given the liability that they may incur if they fail to comply with their obligations under the IP Act, it is recommended that bound CSPs seek independent legal advice as necessary, about how to meet their privacy obligations.

Obligations under the IP Act

The IP Act requires a bound CSP to comply with 10 Queensland Privacy Principles (**QPPs**) set out in schedule 3 of the Act and summarised at the end of this fact sheet.

Overseas disclosure (s33 IP Act)

Bound CSPs are also required to comply with section 33 of the IP Act, which prohibits the disclosure of personal information outside Australia, except in limited circumstances.

Overseas disclosure may occur, for example, if personal information is posted on the internet and accessed from overseas, or if it uses a cloud-based service hosted overseas and the host can access the information.

The standard contract terms require that CSPs seek consent from the department if they intend to send personal information overseas. CSPs must provide evidence of how they will meet their privacy obligations if personal information is disclosed overseas.

The Queensland Office of the Information Commissioner (**OIC**) has published a guideline about overseas disclosure.

QPP codes

Section 41 of the IP Act provides for the development and approval of QPP codes of practice the outline how one or more of the QPPs are to be applied or complied with.

At the date of publication of this fact sheet, there are no approved QPP codes, but CSPs must monitor OIC publications.

Obligations under other legislation

The IP Act is subject to other legislation that may restrict the disclosure of information, e.g. confidentiality provisions in *Child Protection Act 1999*, *Disability Services Act 2006* or *Youth Justice Act 1992*.

The department expects CSPs to be aware of, and comply with, all legislation relevant to their contractual obligations.

Privacy breaches

Privacy breaches may be accidental or deliberate e.g., an email may be sent to the wrong address, or the CSP's computer system could be hacked. They may affect the information of one person or many.

In all cases, it is important that CSPs take immediate containment action and do a risk assessment, so that any potential harm can be prevented or minimised.

The CSP must also notify the department as soon as possible.

Note: IPOLA introduced a Mandatory Data Breach Notification Scheme (**MDBNS**). The scheme does not apply to CSPs, but the department may be required to notify the OIC and affected persons about CSP breaches.

The CSP remains responsible for the breach response, including taking appropriate remedial action and dealing with complaints.

The department will oversee the CSP breach response from a contract management perspective. However, the department cannot provide advice about the breach response, and we recommend CSPs consider seeking independent advice about how to respond.

The OIC has published guidance about how to respond to breaches: Responding to a potential privacy breach | Office of the Information Commissioner Queensland

Privacy complaints

If a person alleges that a bound CSP has breached a QPP, a QPP code or section 33 in relation to their personal information, the CSP must deal with the complaint.

The OIC has published tips for resolving privacy complaints Tips for resolving privacy complaints | Office of the Information Commissioner Queensland

If the complainant is not satisfied with the CSP's response or they do not receive a response within 45 business days, they may refer their complaint to the OIC, who will assess whether the matter can be mediated.

The OIC has published guidance about steps the OIC takes when a complaint is referred to it: Complaints Management Procedure | Office of the Information Commissioner Queensland

If the complainant is not satisfied with the outcome of that process, they may ask the OIC to refer the matter to the Queensland Civil and Administrative Tribunal (**QCAT**) for decision.

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

Because a privacy breach or complaint may expose the CSP to liability, we recommend that CSPs consider seeking independent legal advice, as appropriate.

The Queensland Privacy Principles (QPPs)

The QPPs set out how personal information is to be collected, handled, used and disclosed. A summary of the 10 QPPs is set out below, but you should refer to the IP Act for the full requirements.

Numbering of the QPPs

The QPPs are based on the Australian Privacy Principles (**APPs**) in the federal Privacy Act. The QPPs follow the APP numbering, but not all APPs were adopted. As a result some QPPs, e.g., QPPs 7, 8 and 9 are not used.

QPP1 — Open and transparent management of personal information

QPP1 requires that personal information be managed in an open and transparent way.

You must have a clear, up-to-date and accessible privacy policy, and practices, procedures and systems to ensure QPP compliance.

QPP2 — Anonymity and pseudonymity

QPP2 requires that individuals be allowed the option of not identifying themselves (i.e. to deal with you anonymously or using a pseudonym) unless:

- it is required or authorised under law that you deal with identified persons, or
- it is impracticable to deal with persons who have not identified themselves or who use a pseudonym.

QPP3 — Collection of solicited personal information

QPP3 requires that you:

- only collect personal information that is reasonably necessary for, or directly related to, your functions or activities
- collect it lawfully and fairly, and
- collect it from the individual, unless an exemption applies (e.g. consent, lawful authority or requirement), or it is unreasonable or impracticable to do so.

Higher standards apply to the collection of sensitive information.

QPP3 only applies to solicited personal information, i.e., if you ask someone for it or otherwise takes active steps to acquire it. Unsolicited personal information must be assessed under QPP4.

QPP4 — Dealing with unsolicited personal information

QPP4 requires you to assess unsolicited personal information to determine whether you could have collected it under QPP 3 and/or whether it is a public record.

If not, you may be required to destroy or de-identify the information, subject to the exceptions in QPP4. Otherwise, QPPs 5 to 13 apply to the information.

QPP5 — Notification of the collection of personal information

QPP5 requires you to take reasonable steps to make sure individuals are aware of the matters listed in QPP 5 (e.g. your organisation name and contact details, the fact and circumstances of collection, and the consequences if the information is not collected) when you collect their personal information.

QPP5 applies even if personal information is collected from the person or a third party.

QPP 5 matters can be communicated in many ways, including on a form (hard copy or electronic), in a brochure, or verbally.

QPP6 — Use or disclosure of personal information

You can only use or disclose personal information for the reason it was collected, unless QPP 6 allows it to be used or disclosed for a *secondary purpose*, e.g.:

- if the individual has consented to the use of disclosure of the information
- if QPP 6.2 applies, including where:
  - the individual would reasonably expect you to use or disclose the information for the secondary purpose (unless an exception applies), or
  - the secondary use is required or authorised by law, or reasonably necessary for law enforcement activities, or
- a permitted general situation applies (see schedule 4, part 1, IP Act).

QPP10 — Quality of personal information

QPP10 requires you to take reasonable steps to ensure that:

- the personal information you collect, use, or disclose is accurate, up to date, complete, and
- the personal information is, having regard to the purpose for which it will be used or disclosed, accurate, up to date, complete and relevant.

QPP11 — Security of personal information

QPP11 requires you to take reasonable *steps* to protect personal information you hold from:

- misuse, interference or loss, and
- unauthorised access, modification or disclosure.

You must also take reasonable steps to destroy or de-identify personal information that is no longer needed for any purpose and is not a public record or otherwise required to be retained under law, or court/tribunal order.

QPPs12, 13 — Access to/correction of personal information

QPPs 12 and 13 require you to give access to and correct personal information you hold, subject to listed exceptions.

Note: This guide is based on the OIC's Basic Guide to the Queensland Privacy Principles.

Additional information is available at Information Privacy and Other Legislation Amendment Act | Office of the Information Commissioner Queensland

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances.

For detailed guidance, we recommend that you seek independent legal advice.