

CCC EXHIBIT

7. Privacy Principles

Instructions: Please read the question and enter your response in the space provided.

Question

1.1. What processes does the agency have in place to comply with the Queensland Information Privacy Principles, in particular IPP4 (see below)?:

IPP4:

(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.

QPS Policy on complying with the IPPs is contained in:

- Management Support Manual (MSM) Section 5.7 Release of Information (IPP11)

- MSM s 5.9 Information Privacy Principles - describes the QPS policy requirements for complying with each of the Information Privacy Principles as well as the law enforcement exemptions relevant to the QPS.

- Operational Procedures Manual (OPM) various sections - describes the authority and process for releasing information to other entities.

- Information Management Manual (under review) - describes various aspects of privacy in relation to e.g. information security incident management, QPS Use of Social Media.

Information is available on the QPS Intranet and the QPS External Website on how privacy is managed in the QPS, the IPPs, privacy collection statements, dealing with privacy complaints and breaches, conducting privacy impact assessments.

A Right to Information Online Learning Product describing the requirements of the IPPs and the IP Act is in Ignite. It is compulsory for staff members but not sworn staff. It is under review to separate the RTI and privacy content and approval will be sought to make it compulsory for all staff annually/bi-annually when completed.

The QPS Privacy Team works with new projects and the Enterprise Program Management Office (ePMO) to ensure privacy impact assessments are undertaken on new systems/tools/processes being delivered with a 'privacy by design' approach to ensure the solution complies with the IPPs and the IP Act.

The QPS Privacy Team conducts awareness training to various groups on the IPPs, where to find information about the IPPs, what information they can release, to whom and how, who should approve it, and what to do if they think there has been a privacy breach and/or wish to make a complaint.

The QPS Privacy Team promotes the Office of the Information Commissioner's (OIC) annual Privacy Awareness Week to staff through all staff emails, posters, links to various privacy training opportunity and offers of awareness training etc.

The QPS Privacy Team provides advice to staff on the IPPs, particularly to the use and disclosure of personal information under IPPs 10 and 11, seeking additional advice from the OIC where necessary.

The QPS Privacy Team participates in multi-agency consultation on privacy-related matters such as automated vehicles and the personal information they collect, and how it impacts the QPS and its IPP and other exemptions under the IP Act.

The QPS Privacy Team works with ESC to manage the internal privacy complaint process about possible breaches of the IPPs by the QPS. If a complainant is not satisfied with the QPS response and then goes on to make a privacy complaint to the OIC the Privacy Team works with the OIC to investigate further as to whether a breach of the IPPs has actually occurred. Where a breach of the IPPs is found, the Privacy Team provides advice and guidance to complainants, subject members and relevant business units to prevent a similar incident occurring.

IPPS 1, 2, 3: MSM s 5.9 describes the requirements for collecting person information under IPPs 1-3, including the requirement for privacy collection statements to be included on forms. Information is also available on the QPS Intranet about privacy collections statements. The Privacy Team provides guidance to staff on drafting a collection statement and reviews drafts as necessary.

IPP4: The Information Management Manual provides the policy and standards framework that details how the Services manages its information systems, including the roles and responsibilities of business areas in managing the systems e.g. QPS business areas or PSBA Frontline and Digital Services and actions to be taken when a security incident (data breach) occurs. Many core QPS systems e.g. QPRIME, QCAD, ITAS, have a terms and conditions agreement as part of the login process, requesting the individual to confirm they are accessing the system for a business purpose.

IPP 5, 6, 7: The Right to Information and Privacy Unit administers the scheme that allows individuals to access their own information and request its amendment. Information on the access and amendment scheme is available on the QPS intranet and the QPS External Website.

IPP 8, 9, 10: S 5.9 of the MSM describes the policy requirements for checking the accuracy of personal information before its use, and using personal information only for the relevant purpose.

IPP11: S 5.7 of the MSM describes a wide range of pre-approved arrangements for releasing information about operational policing functions, and for releasing information to e.g. other government entities, law enforcement jurisdictions, members of the public e.g.:

- third party requests for personal information contained in service records

- requests for information related to traffic crashes

- requests by victims of crimes

- information sought by the media

- requests for information from Centrelink

This section also refers to specific sections of the Operational Procedures Manual where other pre-approved arrangements for releasing information are document.

The establishment of these proactive arrangement simplifies the process for the release of information to other entities as the policy for each describes in detail the circumstances under which information can be released, what information, who to, the approval process for releasing the information, and the means of releasing the information.