Office of the Information Commissioner
Queensland

IPOLA

IPOLA RESOURCE

Applying the legislation – Information Privacy Act 2009

Privacy Impact Assessment (PIA)

Risk Considerations

This resource does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This resource does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

This is a companion resource intended to be read in conjunction with the Undertaking a Privacy Impact Assessment and Basic guide to the QPPs guidelines and other resources. It is not a comprehensive guide to identifying or managing privacy risks arising out of a project.

This resource will outline

- common categories of risks
- how these categories relate to the Queensland Privacy Principles (QPPs) and other obligations in the *Information Privacy Act 2009* (IP Act)
- three types of controls to manage these risks.

A range of PIA resources are available to support agencies meet their legislative obligations.

- IPOLA Resource – PIA Threshold assessment Form
- IPOLA Resource – PIA Report Template
- IPOLA Guideline – Undertaking a Privacy Impact Assessment

Common privacy risks

The following tables outline areas of risk that should be considered and managed during a project or when an agency changes how it operates, and the related legislative sections.

Collection risks	
QPP 2	No consideration given to whether it's lawful and practical for people to interact anonymously or pseudonymously with the project. No system in place to facilitate anonymous or pseudonymous interaction.
QPP 3.1	Collecting more personal information than needed, e.g. extra information not needed for the project or information which has nothing to do with the agency's functions/activities.
QPP 3.3	Collecting sensitive information without consent where QPP 3.4 doesn't apply.
QPP 3.6	Collecting personal information from someone other than the individual it is about where QPP 3.6(a) and (b) don't apply.
QPP 4	No system in place to identify and assess unsolicited personal information, e.g. included in free text fields or sent by email.
QPP 5	Not informing people of all the relevant matters listed in QPP 5.2.
Refer to Key privacy concepts – personal and sensitive information, QPP 2 – dealing anonymously and pseudonymously with an agency, QPP 3 – collection of solicited personal information, QPP 4 – dealing with unsolicited personal information, and QPP 5 – informing people when collecting personal information.	

Use and disclosure risks	
QPP 6	Using or disclosing personal information for a secondary purpose (i.e. for something other than why it was collected) without making sure it is permitted by QPP 6.1(a) or QPP 6.2.
Section 33	Disclosing personal information out of Australia when not permitted by section 33.
Chapter 2, part 3	Not taking reasonable steps to bind contractors involved in the project to comply with the IP Act.
Refer to Key privacy concepts – use and disclosure, Disclosing personal information out of Australia, QPP 6 - use or disclosure, and Binding contractors to the IP Act.	

Security and accuracy risks	
QPP 10.1	Not having systems in place to ensure that personal information collected by the project is accurate, up to date and complete. Note: This is primarily a risk when personal information is collected from someone else, instead of from the individual it is about.
QPP 10.2	Not having systems in place to ensure that personal information used and disclosed by the project is accurate, up to date, complete and relevant to whatever is being done with it.
QPP 11.1	Security, systems, practices and access controls are not appropriate to protect personal information from misuse, interference or loss and from unauthorised access, modification or disclosure. Protections must consider both internal and external actors.
QPP 11.2	No systems in place to identify when personal information is no longer needed for any purpose and trigger an assessment about its retention or de-identification.
Refer to QPP 10 – quality and accuracy of personal information and QPP 11 – security, deidentification and destruction of personal information.	

Accountability risks	
QPP 1	Not assessing whether the project must be included in the agency's QPP privacy policy.
Chapter 3A	No systems to identify data breaches arising from the project. No systems to inform internal stakeholders of data breaches and undertake mandatory data breach notification.
Chapter 5	No processes in place to manage privacy complaints arising out of the project.
QPP 12&13	Systems do not support or allow the extraction of personal information into a generic format, for example, a text file or PDF. Systems do not allow personal information to be easily updated by amendment or notation. Note: this is also an important requirement for meeting the agency's obligations under the *Right to Information Act 2009* (Qld).
Refer to QPP 1 – QPP privacy policies, Mandatory notification of data breach scheme, Tips for resolving privacy complaints, and QPP 12&13 – access and correction under the QPPs.	

How to minimise privacy risks

The following tables look at three key ways to mitigate risk; physical barriers, systems and procedures.

Implementing physical security measures	
Physical security measures focus on physical access and control mechanisms, including:	
✓	prohibiting public access to areas where personal information is stored
✓	providing meeting rooms where no information is stored and confidential discussions can take place
✓	implementing a clean desk policy and providing lockable drawers or cabinets
✓	limiting staff access to floors and areas where personal information is stored
✓	limit or prohibit removing hard copy personal information documents from agency premises
✓	implementing organisational sign-in procedures which don’t disclose previous visitors to the premises.

Implementing technical solutions	
Technical solutions focus on minimising privacy risk through technological measures, including through the:	
✓	use and monitoring of audit systems which record access to or alteration of personal information, including by who and when
✓	conduct of threat and risk assessments
✓	control of portable storage device and Bring Your Own Device (BYOD) use through technical controls, policy and training
✓	management of the security and use of agency devices and access to agency systems in a remote work environment using technical controls, policy, and training
✓	use of password protected screen savers
✓	ensuring access privileges and control rights are regularly reviewed and updated
✓	removal of unnecessary data collection fields from systems
✓	assessing the need for collection cookies on the agency website and where it is necessary, providing users with appropriate privacy information.

<table>
<tr><th colspan="2">Implementing privacy positive policies or procedures</th></tr>
<tr><td colspan="2">Develop and put into practice policies or procedures that support privacy awareness and compliance with the privacy principles. This could include policies and procedures:</td></tr>
<tr><td>✓</td><td>limiting and managing the use of portable storage devices and BYOD</td></tr>
<tr><td>✓</td><td>setting agency requirements for staff when working from home, including security of information and devices</td></tr>
<tr><td>✓</td><td>which provide for, and inform staff of, the monitoring and regular review of data access and editing privileges, including information about the consequences of misuse</td></tr>
<tr><td>✓</td><td>which ensure compliance with records management and IP Act requirements such as disposal or deidentification of personal information and disposal or destruction of equipment storing personal information</td></tr>
<tr><td>✓</td><td>for dealing with the post, e.g. sending sensitive personal information by person to person registered post, taking care that only the postal details can be seen when using windowed envelopes, and providing information on the agency website, rather than requiring people to contact the agency and ask for it to be posted</td></tr>
<tr><td>✓</td><td>about collecting personal and sensitive information. This could include guidance on age ranges or year of birth instead of date of birth, requesting a postal address instead of a street address, and sighting identity documents, such as drivers license, rather than making a copy</td></tr>
<tr><td>✓</td><td>that recognise and address the privacy vulnerabilities which exist in some business units, such as web content or social media managers and customer contact staff</td></tr>
<tr><td>✓</td><td>to ensure the agency’s QPP privacy policy is consistent and accessible as required by QPP 1</td></tr>
<tr><td>✓</td><td>for contracts and contract renewals, including chapter 2, part 3 IP Act compliance and contractual protections for personal information.</td></tr>
</table>

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC’s guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published January 2025 and Last Updated 6 January 2025