

Queensland Building and Construction Commission Privacy Management Framework

19 June 2025



Table of Contents

1. PURPOSE.....	4
1.1. The Framework.....	4
2. STRATEGY.....	5
2.1. Vision.....	5
2.2. Objectives.....	5
3. VALUES.....	5
4. SCOPE AND IMPLEMENTATION.....	6
4.1. Scope.....	6
4.2. Application.....	6
4.3. Implementation.....	6
5. PRIVACY MANAGEMENT PRINCIPLES.....	6
6. ROLES AND RESPONSIBILITIES.....	7
7. PRIVACY PRACTICES.....	12
7.1. Transparency of privacy practices.....	12
7.2. Collection, use, and disclosure of personal information.....	12
7.3. Information security and management.....	13
7.4. Access and amendment rights.....	13
7.5. Privacy complaint management.....	14
7.6. Data breach management.....	14
7.7. Privacy risk management.....	15
7.7.1. Privacy by Design.....	16
7.7.2. Third-party risk.....	16
7.8. Employee awareness and training.....	16
8. MONITORING.....	17
8.1. Continual improvement.....	17
8.2. Monitoring and review.....	17
9. DOCUMENT REVIEW.....	18
10. RELEVANT LEGISLATION.....	18

QBCC acknowledges the Aboriginal and Torres Strait Islander Traditional Custodians of Country throughout Australia and recognise the continuing connection to lands, water and communities. We pay our respect to Aboriginal and Torres Strait Islander cultures and to Elders past and present.



Document Control

DOCUMENT INFORMATION

FILE NAME	Privacy Management Framework
DOCUMENT OWNER	Chief Legal Officer
AUTHOR	Director Right to Information and Privacy
APPROVER	Queensland Building and Construction Board
EFFECTIVE DATE	1 July 2025
REVIEW DATE	July 2026

DOCUMENT HISTORY

VERSION	ISSUE DATE	CHANGES
0.1	November 2024	Initial Draft
0.2	December 2024	Revised draft, incorporating SLT feedback
0.3	March 2025	Revised draft, incorporating stakeholder feedback
1.0	June 2025	Release version

SECURITY CLASSIFICATION

CLASSIFICATION	OFFICIAL: Public - No Business Impact
USE	This document is accessible to anyone who requests to view it for the purpose of promoting public awareness of the QBCC's privacy obligations and principles.
PRINTING	The current electronic copy is considered a true version of any controlled document. Uncontrolled hard copies (e.g., printouts) are to be considered a point in time reference only.

DOCUMENT GOVERNANCE

Information Privacy Act 2009 (Qld)

Right to Information Act 2009 (Qld)

Human Rights Act 2019 (Qld)

Information Privacy and Other Legislation Amendment Act 2023 (Qld)

Queensland Building and Construction Commission Privacy Policy

Queensland Building and Construction Commission Data Breach Policy

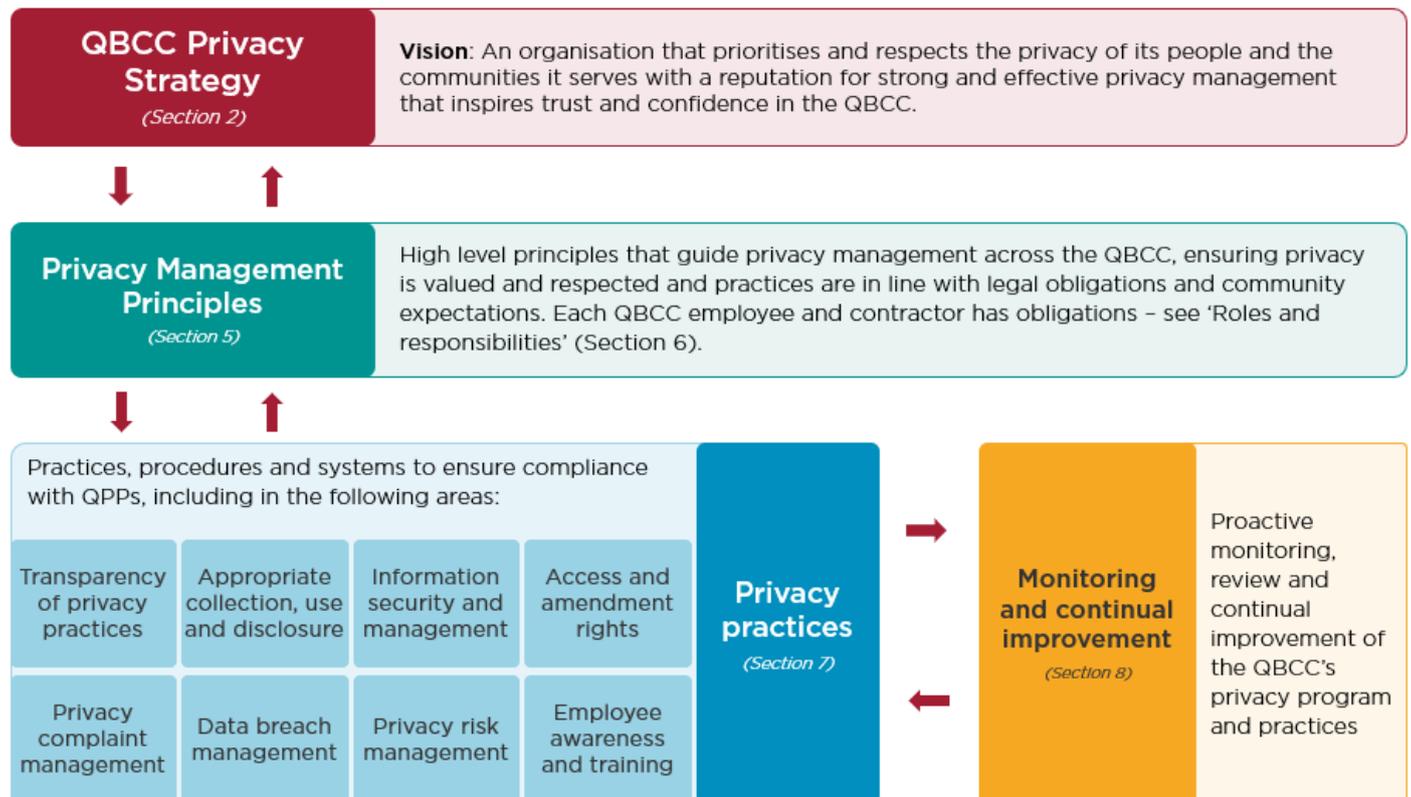
1. Purpose

Personal information (PI) is one of the most valuable business assets of an organisation. The Privacy Management Framework (Framework) outlines how the Queensland Building and Construction Commission (QBCC) prioritises Privacy and fulfills its commitment to complying with the *Information Privacy Act 2009* (Qld) (IP Act).

1.1. The Framework

The Framework is centred around four key components:

Figure 1: Privacy Management Framework components



The Queensland Building and Construction (QBC) Board approves the Framework.

Terms used within the Framework are defined in the Glossary at [Appendix A](#).

2. Strategy

The QBCC acknowledges ‘privacy trust’ as a core expectation from members of the public and its people. As such, the QBCC is transparent about how it handles its PI, providing the right information and offering clear privacy choices that empower them to protect their privacy. QBCC policies and practices uphold the fundamental human right to privacy while enabling innovation and economic growth.

The Privacy Strategy sets the QBCC’s direction, outlining its vision and strategic objectives for building privacy capability and performance. It also supports the establishment of open and transparent dialogue with the public and our people regarding privacy.

2.1. Vision

An organisation that prioritises and respects the privacy of its people and the communities it serves, with a reputation for strong and effective privacy management that inspires trust and confidence in the QBCC.

2.2. Objectives

1. Be an organisation where QBCC people know what their role and responsibility are concerning privacy.
2. Embed a culture that prioritises privacy through leaders who role model respectful and safe handling of privacy practices and empower their people to proactively report all privacy incidents.
3. Educate and inform its people and customers about protecting PI to support continuous improvement and reduce risk and harm.

3. Values

The QBCC is committed to good privacy practices, which is a precondition for the success of an innovative economy and gaining customer and employee trust and confidence. This approach supports effective customer service while safeguarding PI, ensuring an individual’s right to privacy is valued and respected.

The Framework focuses on the foundations of good privacy compliance, which links to QBCC values in the following ways:



Pursue Excellence – The QBCC is a leader in privacy through the implementation of best practice processes and policies to support its people at all levels of the organisation.



Value Customers – The QBCC recognises that trust is increased when good privacy practices are deeply embedded, and all employees know their responsibilities.



Be Courageous – Everyone at the QBCC plays a role in speaking up and managing privacy risk, protecting customer and employee PI, and being accountable for upholding the fundamental human right to privacy.

4. Scope and implementation

4.1. Scope

The Framework sets the direction for building privacy capability and performance across the organisation and supports the QBCC in complying with the IP Act, HR Act, and the *Privacy Act 1988* (Cth).

The Framework addresses IP Act amendments, resulting from the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (IPLA).

4.2. Application

The Framework applies to all QBCC employees and contractors when handling or otherwise dealing with the PI of an individual (including customers).

4.3. Implementation

The QBCC Privacy Team leads the Framework implementation, while supporting the development and promotion of an organisational culture that respects and protects PI. Through leadership support, sufficient resources will be allocated, and planning activities undertaken, with implementation expected to be complete by 30 June 2026.

Privacy-related artefacts to be established are indicated with asterisks (**).¹

5. Privacy management principles

The QBCC acknowledges that PI must be managed appropriately, respected, and protected in line with its legal obligations and community expectations.

The QBCC takes reasonable steps to comply with the IP Act when dealing with PI and strives to meet the expectations of the community by:

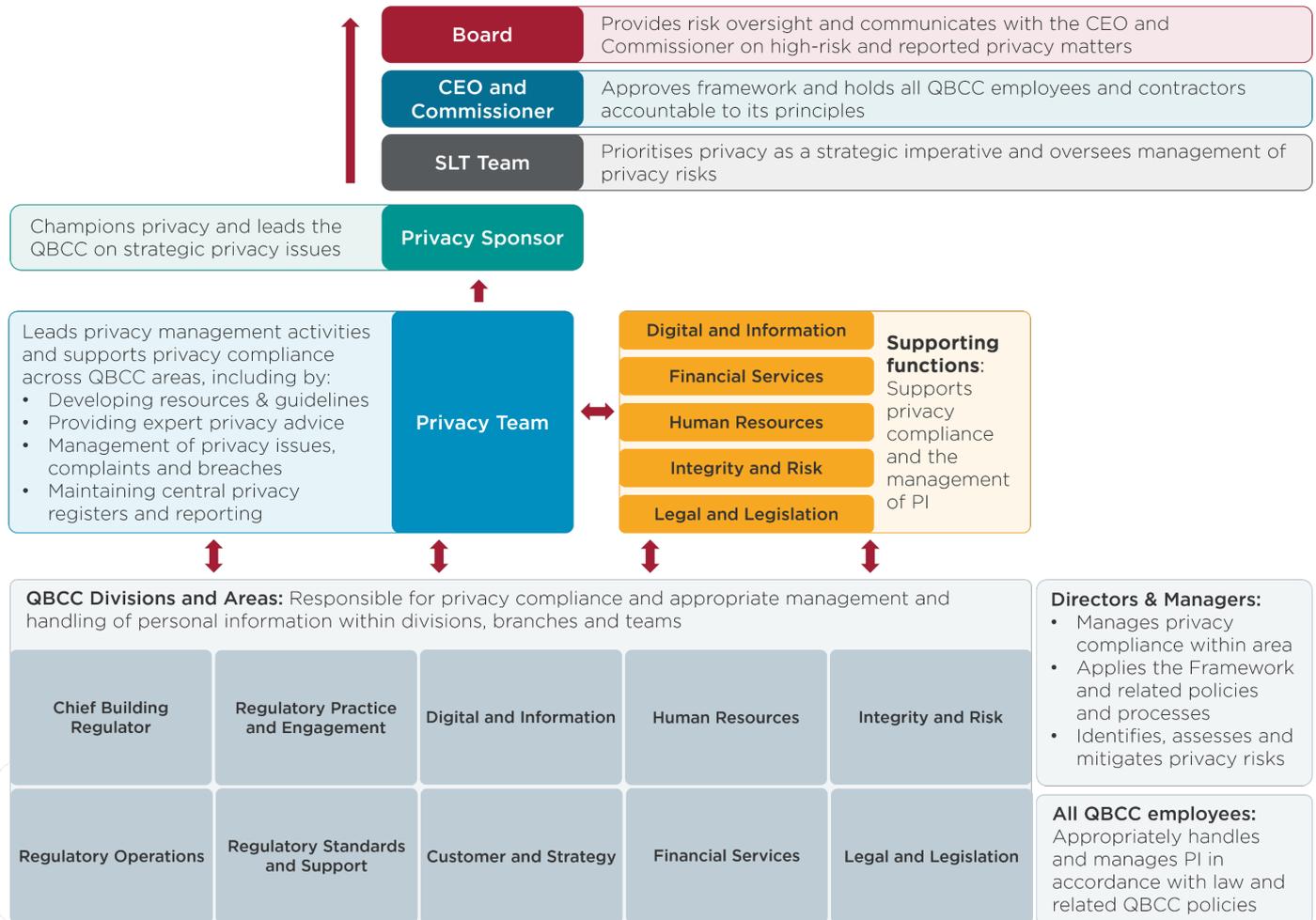
- being clear and transparent about the purposes for which PI is being collected.
- Implementing reasonable technical, administrative, and physical measures to secure PI as part of the Information Security Management System (ISMS).
- taking reasonable steps to carefully deal with PI to avoid disclosure that is not permitted.
- Undertaking due diligence concerning the privacy controls of third-party providers and binding contracted service providers to its privacy obligations under the IP Act.
- monitoring regulatory change and providing privacy advice and training to employees.
- Sufficient allocation of resources to proactively manage privacy across the QBCC.
- taking steps to respond to and investigate known or suspected privacy breaches and data breaches.
- regularly monitoring and reviewing privacy processes, policies, and notices, to keep them up to date, to check they meet legislative, policy, and operational requirements, and to monitor that they are being followed.
- Documenting compliance with privacy obligations, including keeping records of privacy process reviews, breaches, and complaints.
- Implementing reporting mechanisms to inform senior management about relevant privacy issues.

¹ At the time of writing, some privacy-related artefacts were still under development and/or consultation.

6. Roles and responsibilities

The QBCC is committed to ensuring that an individual’s privacy is everyone’s responsibility. The below figure illustrates, at a high level, how privacy is managed at QBCC.

Figure 2: Privacy governance hierarchy at the QBCC



Roles and responsibilities have been defined in the following table to establish accountability for the protection and management of PI held by the QBCC.

ROLE	RESPONSIBILITIES
Board Members	<ul style="list-style-type: none"> • Set the risk appetite in relation to privacy governance for the organisation.
Chief Executive Officer (CEO) and Commissioner	<ul style="list-style-type: none"> • Make respecting privacy and protecting PI a priority for the organisation and approve a framework for it to succeed. • Appoint and resource a Privacy Team with sufficient skills and expertise in regulatory compliance, PI handling and protection, customer and stakeholder liaisons and complaint and access request management. • Ensure the actions and messaging of the Senior Leadership Team clearly demonstrate to staff that the organisation values privacy and protecting PI by adhering to the principles of the Framework.
Senior Leadership Team	<ul style="list-style-type: none"> • Endorse the Framework. • Appoint a Senior Leader as a “Privacy Sponsor” with the purpose of supporting the Privacy Team and championing privacy principles across the organisation.

ROLE	RESPONSIBILITIES
	<ul style="list-style-type: none"> • Model best practice privacy behaviours and ensure respect for the privacy of individuals is part of the organisational culture. • Support the allocation of appropriate resources to support the implementation of and compliance with the Framework. • Support the establishment and operation of a Breach Response Team. • Support the appropriate allocation of resources to support the development and implementation of a privacy management plan that aligns business processes with privacy obligations. • Take all reasonable steps to oversee compliance with the Framework. • Adopt a 'Privacy by Design' (PbD) approach to business activities and decisions that involve PI. • Include PI handling standards in business plans and service standards, including allocating financial resources to support responding to substantiated privacy breaches or complaints.
Privacy Sponsor	<ul style="list-style-type: none"> • Encourage business alignment with the risk appetite and strategic direction concerning privacy governance. • Model best practice privacy behaviours and champion privacy principles across the organisation. • Report on privacy management compliance to the Senior Leadership Team and the Queensland Building Commission Board. • Proactively collaborate with the other areas of the organisation in support of achieving these responsibilities. • Represent the QBCC where a Whole of Government approach to managing significant privacy or data breaches is required/being coordinated.
Directors and Managers	<ul style="list-style-type: none"> • Responsible for privacy compliance and application of the Framework and Privacy Policy to PI collected, stored, used, or disclosed by their respective business area. • Model best practice behaviours by demonstrating sound judgement in privacy matters. • Promote and comply with the Framework, including by undertaking Privacy Impact Assessments (PIAs) where appropriate and adopting a PbD approach. • Identify and manage operational privacy risks. • Ensure privacy breaches, data breaches, incidents, and non-compliances are accurately recorded and reported to the Privacy Team, Director Right to Information (RTI) & Privacy, or Chief Legal Officer, as appropriate. • Support privacy investigations. • Ensure employees receive appropriate privacy training and awareness and encourage staff to report all potential privacy and/or data breaches to the Privacy Team, Director RTI & Privacy, or Chief Legal Officer, as appropriate. • Proactively collaborate with the other areas of the organisation in support of achieving these responsibilities.
Privacy Team	<ul style="list-style-type: none"> • Manage and update the Framework in accordance with legislative requirements and strategic direction. • Lead the implementation of the Framework across the QBCC. • Develop, implement, and undertake a regular review of privacy-related policies, processes, guidelines, templates, and other resources, and provide support for implementation in business areas. • Support business areas to develop, implement, and review privacy collection notices. • Provide expert advice and support to business areas to ensure compliance with the IP Act and the Framework. • Promote a culture of respect for privacy and protection of PI.

ROLE	RESPONSIBILITIES
	<ul style="list-style-type: none"> Promote PI integrity (i.e., importance of maintaining accurate and up-to-date PI and regular culling of PI holdings, as appropriate). Respond to privacy-related enquiries. Raise awareness of, and provide training in, the QBCC privacy obligations (including upcoming amendments to the IP Act) and the Framework. Receive and manage the resolution of privacy-related complaints made to the QBCC. Oversee the management of privacy breaches and data breaches involving PI, including maintaining a central register and undertaking assessments under the Mandatory Notification of Data Breach (MNDB) Scheme. Managing and updating the QBCC Data Breach Policy and associated Data Breach Response Plan. Provide guidance and support relating to privacy risk identification and management. Provide advice and support for the completion of PIAs for new processes or renewed contracts that involve PI. Provide support to the QBCC about undertaking privacy assessments associated with third-party contracted service providers during the procurement process and contract lifecycle. Support the RTI Team to respond to applications for access or amendment of an individual's PI, including employee applications. Proactively collaborate with the other areas of the organisation in support of achieving these responsibilities, including being an active member in internal and external information security and management forums. Manage the engagement of independent privacy assessments and audits (supported by the Regulatory Assurance and Audit Team), when agreed on by stakeholders. Liaise with and respond to audit and information requests from external stakeholders such as the Information Commissioner. Monitor and report on privacy management compliance and uplift activities to the Privacy Sponsor.
Governance and Risk	<ul style="list-style-type: none"> Support the development and implementation of business continuity and critical incident management processes to ensure a coordinated response to a crisis event, including a privacy or data breach threat. This includes collaborating with relevant teams to clarify roles, responsibilities, and escalation pathways to enhance preparedness and response effectiveness. In conjunction with Directors and Managers, provide support in the identification of privacy risks and compliance obligations. Advise on the integration of privacy risk management into the QBCC's Risk Management Framework. Proactively collaborate with the other areas of the business in support of achieving these responsibilities.
RTI	<ul style="list-style-type: none"> Establish, manage, and update the Information Access Framework and lead the implementation and socialisation of the Framework across the QBCC. Deal with access and amendment applications made to the QBCC in accordance with legislative requirements.
Ethics, Standard and Complaints	<ul style="list-style-type: none"> Management and coordination of public sector administrative investigations about corrupt conduct and misconduct matters involving QBCC employees, including unauthorised access or disclosure of PI. Works with the Privacy Team during privacy complaint and breach investigations to ensure a holistic approach.
Regulatory Assurance and Audit	<ul style="list-style-type: none"> Support internal audits of the QBCC's privacy program. Proactively collaborate with the other areas of the business in support of achieving these responsibilities.

ROLE	RESPONSIBILITIES
Legal Services	<ul style="list-style-type: none"> • Advise on confidentiality and privacy-related matters and instances as appropriate and as required. • Where requested, and in consultation with Procurement, provide advice as part of the contract development process to ensure privacy protections are appropriately considered. • Proactively collaborate with the other areas of the business in support of achieving these responsibilities.
Information Management	<ul style="list-style-type: none"> • Maintain the QBCC's Information and Data Governance Framework, Information Asset Register, and publication of QBCC data on the Queensland Government Open Data Portal. • Support the QBCC to ensure records are retained, stored, and destroyed in accordance with the <i>Public Records Act 2023</i> (Qld) (PRA) • Proactively collaborate with the other areas of the business in support of achieving these responsibilities.
Digital Services	<ul style="list-style-type: none"> • Implement, maintain, and continually improve an ISMS that aligns with ISO 27001 to ensure appropriate controls are in place to secure PI held by the QBCC. • Proactively consider, and make decisions as to, when security access controls are developed, implemented, maintained, and monitored. • Undertake cyber-security assessments concerning third-party contracted service providers of ICT applications, solutions, and services during the procurement process and contract lifecycle. • Proactively manage the security of all data and information on the QBCC network from accidental and malicious access. • Provide expert advice in the information security aspects of PIAs. • Proactively collaborate with the other areas of the business in support of achieving these responsibilities.
Procurement	<ul style="list-style-type: none"> • Ensure procurement processes include steps to manage third-party privacy risks by incorporating privacy considerations into procurement procedures, templates, and guidance tools. This includes steps to ensure: <ul style="list-style-type: none"> • Privacy risk assessments are undertaken as part of due diligence activities • Privacy is appropriately considered and addressed in the contract development process • Ongoing management of suppliers by conducting privacy and security-related reviews • Personal information is returned and destroyed upon contract expiry or termination, per contractual requirements. • Monitor contract manager adherence to procurement procedures and required steps. • Co-operate with the other areas of the business in support of achieving these responsibilities.
Enterprise Portfolio Management Office and Digital Portfolio Office	<ul style="list-style-type: none"> • Ensure project management processes for digital and non-digital projects include steps to consider privacy impacts and apply a PbD approach, and where required, ensure a PIA is conducted at the design and development phases. • Co-operate with the other areas of the business in support of achieving these responsibilities.
All employees	<ul style="list-style-type: none"> • Comply with the Framework, including by undertaking PIAs before commencing activities or operations that are likely to impact the privacy of individuals, i.e., where PI is involved. • Actively participate in privacy training and awareness programs, including completing mandatory and refresher privacy training. • Comply with all information security, information management, and privacy policies and procedures, including by only accessing PI for business-related and role-specific purposes. • Cooperate fully with any privacy investigation.

ROLE	RESPONSIBILITIES
	<ul style="list-style-type: none">• Report all known or suspected privacy breaches, data breaches, incidents, or complaints to their Manager or Leader.• Proactively collaborate with the other areas of the business in support of achieving these responsibilities.

7. Privacy practices

The QBCC is committed to taking all reasonable steps to implement practices, procedures, and systems to ensure compliance with the privacy principles in the IP Act, and to ensure it can deal with inquiries and complaints about its compliance. This section details the practices, procedures, and systems in place to manage privacy and protect PI.

7.1. Transparency of privacy practices

The QBCC is open and transparent about its management of privacy and its PI handling practices. As such, the QBCC's external Privacy Policy:

- is easily accessible via the QBCC website.
- is clearly expressed and written using plain language.
- is up-to-date and accurately reflects the QBCC's current practices.
- provides sufficient information to ensure the public and our people are informed about how the QBCC collects, stores, uses, discloses, and provides access to PI.

The QBCC further promotes public awareness of its privacy obligations and principles by:

- making the Framework and associated policies accessible to anyone who requests to view them.
- Resourcing a dedicated Privacy Manager and Privacy Team to respond to and manage privacy-related enquiries, issues, and complaints.

Reference documents	**QBCC Privacy Policy **Privacy Notice Guide and Template **Privacy Management Plan
---------------------	---

7.2. Collection, use, and disclosure of personal information

The QBCC collects, uses, and discloses PI in accordance with the privacy principles in the IP Act. Importantly, the QBCC and its employees:

- **Restrict internal sharing** of PI unless the information is to be used for the same purpose for which the information was collected.
- **Limit the use and disclosure** of PI for the purpose for which the PI was collected and not for any other purpose unless permitted.
- Apply a **data minimisation** approach, restricting the collection of PI to only that which is necessary for the purpose of collection.
- **Notify** individuals about the collection of PI, ensuring individuals are aware of certain matters at or before the time of collection, including the purpose of collection, whether the collection is required or authorised by law, and usual disclosures of PI of the kind collected.
- Collect PI by **lawful and fair means**, and not by trickery, deception, or misleading conduct.
- Take reasonable steps to ensure the **quality** of PI collected, used, and disclosed to ensure it is accurate, complete, and up to date.
- Provide individuals with the option of remaining **anonymous** or using a pseudonym where practicable.

Reference documents	**Privacy intranet page Camera Surveillance Policy Information and Data Sharing Guideline
---------------------	---

7.3. Information security and management

The QBCC takes all reasonable steps to ensure PI is secured and appropriately managed throughout the information lifecycle (i.e., from collection to destruction).

As such, the QBCC:

- Maintains an ISMS that aligns with ISO 27001, to ensure appropriate security controls are in place to ensure the confidentiality, integrity, and availability of PI.
- Adheres to the Information and Data Governance Framework that provides an enterprise approach to governance of all information and data held by the QBCC (including PI).
- Retains and stores records containing PI in accordance with the PRA.
- Destroys or de-identifies records retaining PI in accordance with the PRA and relevant Retention and Disposal Schedules, ensuring that PI is not retained longer than necessary.

Reference documents	Information Security Management System Framework Cyber Security Strategy Cyber Security Policy **Auxiliary Cyber Documentation Suite Information and Data Governance Framework and Operating Model Information Management Policy QBCC Retention and Disposal Schedule General Retention and Disposal Schedule (GRDS)
---------------------	---

7.4. Access and amendment rights

Under Queensland's information privacy and access framework, an individual has a right to access or amend their PI that the QBCC holds about them, free of charge.

Informal requests: Most PI requests are handled informally, or outside of the formal application process (e.g., formal applications made under the RTI Act). QBCC employees follow the Administrative Access Policy to ensure PI requests are received and addressed expediently and appropriately, in line with privacy principles and the 'push model' established under the RTI Act. The QBCC further provides self-service avenues where individuals can automatically access and amend their PI (such as via myQBCC or the QBCC's human resources platform).

Formal applications: An individual can make a formal access or amendment application for PI at any time. The QBCC provides clear processes and avenues for individuals to submit a formal application (i.e., via the [Accessing information held by QBCC](#) webpage). Team members in the QBCC RTI Team have been delegated power under the RTI Act to deal with formal applications.

Formal applications for access to another individual's PI made under the RTI Act are submitted in the same manner. The QBCC RTI Team will assess applications on a case-by-case basis, considering whether the requested PI is exempt information or whether releasing the information is contrary to the public interest.

Internal review: The QBCC supports an individual's right to apply for an internal review if they are not satisfied with a decision regarding their formal application - i.e., where the decision is a 'reviewable decision' as defined under the RTI Act (e.g., a decision refusing access to a document). Authorised members of the QBCC RTI Team will conduct a review of the decision in accordance with the RTI Act.

External review: The QBCC further cooperates with the Office of the Information Commissioner (OIC) where an individual has submitted an external review application with the OIC.

Reference documents	<ul style="list-style-type: none"> **Privacy Policy **Accessing information held by QBCC webpage **Information Access Framework **Administrative Access Policy
---------------------	--

7.5. Privacy complaint management

The QBCC encourages and supports its employees to raise privacy-related issues, concerns, and complaints with their Managers, Leaders, or the QBCC Privacy Team. The QBCC commits to dealing with complaints well and developing a strong reputation for being a trusted Regulator and utilising learnings to improve its privacy practices.

The QBCC deals with all privacy complaints regardless of how they are received. This includes privacy complaints received via the QBCC contact centre, the online feedback form, the QBCC RTI or Privacy mailbox, or via the OIC. The QBCC investigates and responds to complaints efficiently and effectively, within 45 business days of receiving the complaint (unless additional time is requested and agreed upon).

Complaints that are not resolved at the first point of contact are referred to the Privacy Team for investigation, management, and response. The Privacy Team are otherwise notified of resolved complaints to ensure a central record of all privacy complaints received by the QBCC is maintained.

Where a privacy breach is identified as a result of an investigation into a privacy complaint, the QBCC implements mitigating steps to reduce the likelihood of a similar privacy breach occurring in the future.

OIC Mediation services: Where the complainant is not satisfied with the QBCC’s response and brings the complaint to the OIC, the QBCC will participate in mediation with the complainant under the facilitation of the OIC and provide all information relevant to the OIC’s mediation service for privacy complaints.²

Queensland Civil and Administrative Tribunal (QCAT): When resolution of a complaint cannot be achieved through mediation, and a complainant refers the complaint to QCAT, the QBCC may engage appropriate legal counsel, financial/insurance, and/or other expert advice (e.g., industrial relations advice) in a timely manner to support the QBCC’s approach.

Reference documents	<ul style="list-style-type: none"> **Privacy Policy **Privacy Complaint Management Guideline Privacy Complaint Register Customer Feedback Policy [under review] Individual Employee Grievance Policy and Procedure
---------------------	---

7.6. Data breach management

A robust data breach response procedure is essential for protecting PI and minimising impact in the event of a data breach, including reducing harm to affected individuals and impacts to the QBCC (e.g., financial, reputational, and non-compliance impacts). In the event of a data breach that involves PI, the QBCC will take all reasonable steps to investigate and restore compliance with the IP Act and the Framework.

² It is noted that privacy complaints may also be referred to the OIC by entities such as the Ombudsman or any other commission or external review body that has received a privacy complaint through the performance of its functions under law.

The Privacy Team collaborates with the Digital and Information division to ensure alignment with security incident response processes. Key components of the QBCC's data breach preparation and response include:

- **Accountability:** Publication of a Data Breach Policy on the QBCC website, which sets out how the QBCC will respond to a data breach.
- **Data Breach Response Plan:** Implementation of a Data Breach Response Plan that provides overarching steps for managing a data breach that involves PI, including steps to:
 - Contain the breach and prevent further data loss.
 - Assess the breach, risk of harm, and possibility of remediation.
 - Notify relevant parties, including other agencies affected by the breach, the Information Commissioner, and affected individuals.
 - Review the QBCC's response and consider actions to prevent future breaches.
- **Data Breach Response Team:** Designation of a cross-functional team led by the Privacy Sponsor (supported by the Director RTI and Privacy) to oversee breach response efforts that includes stakeholders from:
 - Privacy
 - Finance
 - Digital Services
 - Information Management
 - Legal Services
 - Governance, Risk, and Ethics
 - Communication and Executive Services
 - Human Resources
- **Notification:** Customer-focused approach to notification that emphasises clear, timely, and empathic communication with individuals affected by an eligible data breach.
- **Training and awareness:** Implementation of regular training and awareness sessions for all employees to recognise and report known or suspected data breaches that involve PI.
- **Tabletop exercises:** Privacy Team involvement in simulations to test response plans and ensure readiness and familiarity with established, eligible data breach response steps and responsibilities.

By adhering to these key components, the QBCC enhances its resilience against data breaches and ensures continuous improvement in response capabilities.

Reference documents	<ul style="list-style-type: none"> **Data Breach Policy **Data Breach Response Plan **Data Breach Register **Cyber Security Incident Response Plan Critical Incident Management Plan
---------------------	---

7.7. Privacy risk management

The identification, assessment, mitigation, and oversight of privacy-related risks supports privacy compliance and the protection and safeguarding of PI. The QBCC actively identifies privacy-related risks at a strategic, operational, and project level in line with the QBCC Risk Management Framework and Policy. In line with best practice, all QBCC staff will complete a Privacy Impact Assessment (**PIA**) for all new or changed projects, business processes, contracts, engagements, procurement of services, or other business activities where personal information is involved, e.g.,

procuring software that will involve the collection, use, storage of and access to PI, or implementation of an enterprise recordkeeping system. Privacy-specific risks can also be identified through the investigation and review of privacy complaints, privacy breaches (including data breaches that involve PI), near misses, and other issues identified.

Reference documents	Compliance Management Framework Risk Management Framework Risk Management Policy Risk Appetite Statement Risk Matrix
---------------------	--

7.7.1. Privacy by Design

The QBCC promotes [Privacy by Design \(PbD\)](#) principles and embeds privacy into the design and operation of systems, services, products, and business practices. The PbD principles are a best practice approach that builds privacy into decision making, as opposed to being an afterthought.

PbD shifts the focus from compliance to prevention as it supports the QBCC to design, manage, and implement initiatives in a way that respects and protects an individual's privacy rights. As such, the PbD approach supports the QBCC to minimise and manage privacy risks associated with PI handling.

A PIA is a tool that supports the QBCC to proactively understand and mitigate privacy impacts in the design and development of new systems, products, services, and business practices that involve PI. The QBCC is committed to conducting a PIA where there is a new or changed way that PI is handled or managed.

Reference documents	**Privacy Impact Assessment Guideline **Privacy Threshold Assessment Template **Privacy Impact Assessment Template
---------------------	--

7.7.2. Third-party risk

Third-party risk management is a critical component of privacy management at the QBCC, as the involvement of contract service providers can significantly impact privacy and the security of PI.

The QBCC assesses potential third-party privacy risks by conducting thorough due diligence on third-party practices, ensuring adherence to privacy standards and legislative requirements. Further, the QBCC's standard contractual position ensures that any contracted service provider is bound to comply with its privacy obligations under the IP Act.

Ongoing monitoring and audits are implemented to evaluate contracted service provider compliance and PI handling practices, allowing the QBCC to mitigate risks and protect PI effectively.

Reference documents	Procurement Policy Vendor Risk Management Framework Cyber Security Assessment Procedure
---------------------	---

7.8. Employee awareness and training

A program of privacy training and awareness is established and provided to all QBCC employees through various methods, depending on the employees' interactions with PI, such as:

- integration into all staff learning and development processes (i.e., at induction and periodic refresher training)
- face-to-face training and seminars
- online training
- intranet-based information (i.e., via the QBCC privacy intranet page)
- email updates and alerts.

Training and awareness activities educate employees about their privacy and confidentiality obligations under the IP Act, RTI Act, HR Act, *Public Sector Act 2022* (Qld), and the Queensland Public Service Code of Conduct.

Reference documents

[**QBCC Privacy intranet page](#)

**Privacy training and awareness program

8. Monitoring

8.1. Continual improvement

The QBCC conducts a Privacy Maturity Assessment on a biennial basis to assess the agency's privacy maturity, identify compliance gaps, and plan for upcoming privacy management uplift activities.

Actions identified from the Privacy Maturity Assessment will inform the establishment of a Privacy Management Plan (**PMP**), with recorded actions to be completed within 2 years. A PMP identifies specific, measurable privacy goals and targets that set out how the QBCC will strengthen its privacy maturity and its ability to proactively meet its privacy compliance obligations.

8.2. Monitoring and review

The QBCC proactively monitors and reviews its privacy management regularly to ensure it remains relevant and effective. This includes:

- **Framework oversight:** The Privacy Team (supported by the Privacy Sponsor) is responsible for oversight of the Framework and its implementation, and implementation of PMP action items.
- **Annual reviews:** Privacy-related policies, collection notices, privacy training and resources, and PIA templates are reviewed annually to ensure they remain up to date and fit for purpose.
- **Risk review:** Risk owners regularly examine risk registers to ensure effective management of privacy-related risks.
- **Communication of changes:** Material changes to privacy-related policies and practices are communicated to employees and stakeholders.
- **Documentation of compliance:** Records of privacy reviews, breaches, and complaints to identify systemic risks and improvement opportunities are maintained.
- **Feedback mechanism:** A culture of continuous improvement is fostered to encourage suggestions from QBCC employees and stakeholders.
- **Independent assessment and audit:** Assessment of the QBCC's privacy program or specific practices is periodically undertaken by an independent body (such as the outsourced Internal Audit function) to identify areas that may need improvement.

- **Reporting:** The Director RTI and Privacy regularly reports to the Privacy Sponsor and Senior Leadership Team on the progress of the PMP, breaches, complaints, and privacy audits when agreed on by stakeholders.

9. Document review

The Framework is reviewed annually, or after significant legislative changes or organisational shifts, to ensure the Framework remains current, effective, and aligns with QBCC’s strategic objectives and best practices.

10. Relevant Legislation

AREA	LEGISLATION AND REGULATION
Privacy	<ul style="list-style-type: none"> • <i>Information Privacy Act 2009 (Qld)</i> • <i>Information Privacy and Other Legislation Amendment Act 2023 (Qld)</i> • <i>Privacy Act 1988 (Cth)</i>
Human rights	<ul style="list-style-type: none"> • <i>Human Rights Act 2019 (Qld)</i>
Right to information	<ul style="list-style-type: none"> • <i>Right to Information Act 2009 (Qld)</i> • <i>Information Privacy and Other Legislation Amendment Act 2023 (Qld)</i>
Public records	<ul style="list-style-type: none"> • <i>Public Records Act 2023 (Qld)</i>
Public sector employees	<ul style="list-style-type: none"> • <i>Public Sector Act 2022 (Qld)</i> • <i>Code of Conduct for the Queensland Public Service</i>
OTHER LAWS RELEVANT TO THE HANDLING AND MANAGEMENT OF PI IN A PARTICULAR CONTEXT	
QBCC specific laws	<ul style="list-style-type: none"> • <i>Queensland Building and Construction Commission Act 1991 (Qld)</i> • <i>Queensland Building and Construction Commission Regulation 2018 (Qld)</i> • <i>Queensland Building and Construction Commission (Minimum Financial Requirements) Regulation 2018 (Qld)</i> • <i>Queensland Building and Construction Commission (Non-Conforming Building Products Code of Practice) 2017</i>
Building laws	<ul style="list-style-type: none"> • <i>Building Act 1975 (Qld)</i> • <i>Building Regulation 2021 (Qld)</i>
Security of payment	<ul style="list-style-type: none"> • <i>Building Industry Fairness (Security of Payment) Act 2017 (Qld)</i> • <i>Building Industry Fairness (Security of Payment) Regulation 2018 (Qld)</i>
Plumbing and drainage	<ul style="list-style-type: none"> • <i>Plumbing and Drainage Act 2018 (Qld)</i> • <i>Plumbing and Drainage Regulation 2019 (Qld)</i>

Appendix A: Glossary

Terms used within the Framework are defined in the table below.

TERM OR ACRONYM	DEFINITION
Collection	Collection (of PI) refers to how the QBCC acquires PI, which can include collections via a written form, a verbal conversation, a voice recording, or a photograph. The QBCC may also collect PI from other sources, such as from third parties or publicly available sources.
Data breach	The unauthorised access, use, or disclosure of information held by the QBCC or the loss of information in circumstances where unauthorised access or disclosure is likely to occur. This is a distinct type of privacy breach that relates to a failure to secure information (e.g., where a third-party hacker obtains information from the QBCC's systems, or an inadvertent disclosure of PI to another customer).
Disclosure	Disclosure (of PI) occurs when the QBCC gives an individual or entity PI not previously known to them, or places the individual or entity in a position to be able to find out the PI.
Eligible data breach	A data breach that involves PI and is likely to result in serious harm to an individual to whom the PI relates.
Framework	The Privacy Management Framework
IP Act	<i>Information Privacy Act 2009</i> (Qld)
IPOLA	<i>Information Privacy and Other Legislation Amendment Act 2023</i> (Qld)
ISMS	Information Security Management System
ISO 27001	ISO/IEC 27001:2022 Information technology – Security Techniques – Information Security Management Systems – Requirements
MNDB Scheme	The Mandatory Notification of Data Breach Scheme imposes obligations on the QBCC to contain, mitigate, and assess known or suspected eligible data breaches and notify the Information Commissioner and affected individuals.
OIC	Queensland Office of the Information Commissioner
PbD	Privacy by Design (PbD) is a best practice approach where privacy is built into the design, operation, and management of a system or business process. PbD is based on the following seven key principles: <ul style="list-style-type: none"> o proactive not reactive; preventative not remedial o privacy as the default setting o privacy embedded into design o full-functionality – aiming for win-win outcomes as opposed to trade-offs o end-to-end security – full lifecycle protection o visibility and transparency o respect user privacy – keep it user-centric.
PMP	Privacy Management Plan
Personal information (PI)	Personal Information has the meaning set out in the IP Act, being information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: <ul style="list-style-type: none"> o whether the information or opinion is true or not o whether the information or opinion is recorded in a material form or not.
PIA	A privacy impact assessment is a tool to assist with identifying: <ul style="list-style-type: none"> o What PI is involved in a new or changed process o the potential impact on privacy and whether the proposed collection, use and disclosure of PI will comply with the IP Act

TERM OR ACRONYM	DEFINITION
	<ul style="list-style-type: none"> o risks of, and mitigation strategies for, any potential negative impacts.
Privacy breach	An action or activity that directly results in an agency subject to the IP Act, failing to comply with one or more of the privacy principles set out in the IP Act (for example, the use of PI by an employee for a purpose other than that for which the QBCC was permitted).
Privacy complaint	A complaint about the QBCC's collection, use, disclosure, or storage of an individual's PI.
Privacy trust	The confidence the public has in the QBCC to handle their PI responsibly, transparently, and in line with privacy principles, ensuring that privacy protections foster stronger relationships and enable better services.
RTI Act	<i>Right to Information Act 2009 (Qld)</i>
Use	<p>Use (of PI) occurs when the QBCC (a) manipulates, searches or otherwise deals with the information, (b) takes the information into account in the making of a decision, (c) transfers the information from one part of the QBCC to another part of the agency, or (d) other actions that may be a use of PI.</p> <p>The QBCC will not use an individual's PI for a purpose other than for which it was collected, unless it is authorised under the IP Act or other law to do so (such as the individual expressly or impliedly agreed, law enforcement activities, or any purposes directly related to the primary purpose).</p>