Privacy Policy

Queensland Corrective Services

Purpose of this document

As part of day-to-day activities, Queensland Corrective Services (**QCS**) is required to handle personal information. The *Information Privacy Act 2009* (**IP Act**) regulates how QCS and other Queensland Government agencies must handle personal information collected, stored, used, and disclosed in accordance with the Queensland Privacy Principles (**QPPs**)[1].

This document informs QCS employees, volunteers, community members, and other persons or businesses who may provide a service to QCS about:

- the kind of personal information QCS collects and holds;
- how QCS collects and holds personal information;
- the purposes for which QCS collects, holds, uses, and discloses personal information;
- how an individual may access personal information held by QCS, and seek correction of the information;
- how an individual may make a complaint about a breach of the QPPs or any QPP code that binds QCS, and how QCS will deal with the complaint; and
- whether QCS is likely to disclose personal information to entities outside Australia and the countries in which the recipients are likely to be located and, if practicable, state those countries.

Personal information definition

The IP Act section 12 defines personal information as:

> *Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion –*
> *a) whether it is true or not; and*
> *b) whether the information or opinion is recorded in material form or not.*

Queensland Privacy Principles

QCS can only lawfully collect personal information that is reasonably necessary for or directly relates to its functions or activities. QCS is committed to managing personal information in accordance with the below QPPs:[2]

QPP 1 – Open and transparent management of personal information

QCS is required to have an up to date and accessible QPP privacy policy (this document)

---

[1] The QPPs replace the Information Privacy Principles (IPPs) from 1 July 2025.
[2] Schedule 3, Part 1 IP Act. Please note QPPs 7, 8, and 9 are intentionally blank as they are not active.

and implement practices and procedures to ensure QPP compliance.

QPP 2 – Anonymity and pseudonymity

An individual has the option of not identifying themself to QCS, unless it is required or authorised under law, or impracticable.

QPP 3 – Collection of solicited personal information

QCS can only collect personal information lawfully and fairly and if it is reasonably necessary for, or directly related to, one of its functions or activities.

Personal information must be collected directly from the individual, unless an exemption applies[3], or it is unreasonable or impracticable to do so.

In addition, QCS must not collect *sensitive information* unless the individual consents to the collection, a permitted general situation[4] exists, or QCS believes the collection is reasonably necessary. *Sensitive information* is a specific category of personal information and is defined in Schedule 5 of the IP Act.

QPP 4 – Dealing with unsolicited personal information

QCS must assess unsolicited personal information to determine if QCS would have been permitted to collect the personal information in line with one of its functions or activities (QPP 3).

If QCS decides it could not have collected the information under QPP 3 and the information is not contained in a public record[5] QCS must, where lawful and reasonable to do so, destroy or de-identify the information.

QPP 5 – Notification of the collection of personal information

QCS is required to take reasonable steps to provide general information about:

- appropriate contact details;
- the facts and circumstances of the collection e.g. personal information is collected from someone other than the individual;
- any laws which give QCS the authority to collect the information;
- the purpose of the collection;
- consequences if information is not collected;
- to whom QCS usually discloses or gives the information;
- QCS' Privacy Policy, and information it contains;
- if the personal information will be disclosed overseas and the countries in which the recipients are likely to be located and, if practicable, state those countries.

QPP 6 – Use or disclosure of personal information

QCS can only use or disclose personal information for the purpose it was collected unless there is consent to the other purpose, or the secondary purpose is for a legitimate reason.[6] For example, if the use or disclosure is required or authorised under an Australian law or a court or tribunal order.

---

[3] See, generally, section 29 or QPP 3 of the IP Act.
[4] Permitted general situations are stated in schedule 4, part 1 IP Act.
[5] As defined under the *Public Records Act 2023*.
[6] QPP 6.2 IP Act.

QPP 10 – Quality of personal information

QCS must take reasonable steps to ensure:

- the personal information QCS collects is accurate, up to date and complete; and
- the personal information QCS uses or discloses is, having regard to the purpose of the use or disclosure, is accurate, up to date, complete and relevant.

QPP 11 – Security of personal information

QCS is required to take reasonable steps to:

- protect the personal information QCS holds from misuse, interference, loss, unauthorised access, unauthorised modification, or unauthorised disclosure; and
- destroy or deidentify personal information no longer needed for any purpose which is not a public record (as defined by the *Public Records Act 2023*) or otherwise required to be retained under law, court, or tribunal order.

QPP 12 – Access to personal information

Anyone may seek access to their personal information held by QCS through the *Right to Information Act 2009*. Please refer to the Accessing and amending personal information section in this document.

QPP 13 – Correction of personal information

QCS is required to take reasonable steps to correct personal information it holds to ensure it is accurate, up to date, and relevant.

Anyone may seek to correct their personal information held by QCS through the *Right to Information Act 2009*. Please refer to the Accessing and amending personal information section in this document.

QCS as a 'law enforcement agency'

QCS is defined as a *law enforcement agency* for the purposes of the IP Act.[7]

In limited circumstances, QCS is exempt from complying with some of the QPPs[8] when reasonably satisfied noncompliance is necessary for the collection, notice, use and disclosure of personal information, in the administration of:

- the containment, supervision and rehabilitation of offenders under the *Corrective Services Act 2006*; or
- the supervision of prisoners subject to supervision orders or interim supervision orders under the *Dangerous Prisoners (Sexual Offenders) Act 2003*.

For example, QCS collects personal information during the performance of an activity necessary for the safety and security of a correctional facility, and compliance with QPP 5 (notification of the collection of personal information) would endanger the life, health or safety of QCS officers or prisoners.

[7] See Schedule 5 IP Act.
[8] Section 29(1)(c) IP Act.

Kinds of personal information collected and held by QCS

QCS collects and holds personal information that is reasonably necessary for, or directly related to, the performance of QCS functions and activities, and may include an individual's:

- name and signature
- date and place of birth
- photographs, images, CCTV footage
- contact details such as email and residential address
- marital status
- education information
- employment status
- criminal history
- next of kin contact information
- ethnicity and nationality
- religion or philosophical beliefs
- political opinions and/or membership of a political association
- membership of a professional or trade association, or of a trade union
- sexual orientation or practices
- any aliases – known by other name
- medical information including diet
- physical description including height, weight, hair, eye colour and distinguishing marks and tattoos
- biometric information such as fingerprint and eye scanning data
- information about personal and virtual visits to prisoners
- body scan and radiation exposure data
- positive drug screening indication results
- information about any complaints made by or against someone
- information about suppliers of goods and services
- employee information and employment records
- recruitment information
- information provided in response to QCS surveys.

How QCS collects personal information

QCS may collect personal and sensitive information directly from the individual, their representative, or a third party. While personal information is usually collected directly from the individual to whom the information is about, in certain circumstances QCS may also obtain personal information from a third party including other government agencies or organisations.

QCS may collect personal information from third parties in the following circumstances:

- with the individual's consent;
- where it is unreasonable or impractical to collect the information from the individual if required or authorised to do so by law.

QCS collects personal information in a variety of ways. These include:

- directly from the individual (face to face)

- via paper-based forms
- via correspondence and submissions
- via phone calls
- online (including through web-based forms and emails)
- data and other information sharing arrangements with third parties.

How QCS holds personal information

Personal information held by QCS is managed securely through its recordkeeping systems. QCS takes physical and electronic security measures to protect personal information from misuse, interference, and loss; and from unauthorised access, modification, or disclosure.

QCS' electronic records management system, network drives and virtual server environment are hosted by QCS within Australia and secures electronic information using firewalls, secure databases, secure online systems, password protection for electronic files, and/or multi-factor authentication.

QCS restricts physical access to its offices and physical files to authorised persons only.

Staff members across QCS have access to personal information on a need-to-know basis only. Sensitive personal information stored in its databases can only be accessed by authorised users to work on particular enquiries, complaints, applications, and/or cases. These databases have an audit trail whenever personal information is included, amended, or deleted.

When the personal information is no longer required to be retained as part of a public record, the personal information may be destroyed. Any destruction of personal information will be made in accordance with the *Public Records Act 2023*.

Why QCS collects personal information

Personal information is only collected where it is necessary for, or directly related to, the performance of its functions and activities. QCS will not collect any personal information if it doesn't need to. QCS collects personal information:

- for the containment, supervision and rehabilitation of offenders under the *Corrective Services Act 2006*;
- to process an offender's induction into a corrective service facility;
- to ensure the provision of any medical needs required by an offender;
- to administer the probation of offenders;
- during the reintegration (pre release) planning period of an offender;
- for the supervision of offenders subject to supervision orders or interim supervision orders under the *Dangerous Prisoners (Sexual Offenders) Act 2003*;
- to provide safe, modern, and responsive correctional services through the operation of correctional facilities, work camps, and Community Corrections regional and district offices;
- to enhance the safety of Queenslanders through modern, sustainable, and evidence-based corrective services to maximise rehabilitation and reduce recidivism;
- to decide whether a visitor poses a risk to the security or good order of a corrective services facility;

- to process biometric and photographic data for non-offender entry into correctional centres;
- to process security clearances;
- for the management of QCS employees and contracted parties.

How QCS uses and discloses personal information

Generally, QCS must only use or disclose personal information for the purpose it was collected for. In certain circumstances, QCS may use or disclose personal information for a secondary purpose, including where one or more of the following applies:

- the individual has consented to the use or disclosure for a secondary purpose; or
- the individual would reasonably expect QCS to use the information for that other purpose; or
- it is legally required or authorised, by or under an Australian law, or court or tribunal order; or
- it is reasonably necessary for an enforcement-related activity conducted by, or on behalf of, an enforcement body; or
- QCS reasonably believes it is necessary to lessen or prevent a serious threat to the life, health, or safety of any individual, or to public health or safety.

The third parties QCS may disclose personal information to, or who may collect personal information on QCS' behalf, include but are not limited to suppliers and other third parties (for example, external psychologists, other government agencies, and research institutions). QCS must ensure appropriate protections of personal information are in place with the third parties, consistent with its obligations under the IP Act.

Accessing and amending personal information

Anyone can apply to access their personal information held by QCS and apply to amend or correct their personal information, by making a formal request for access or amendment under the *Right to Information Act 2009*.[9]

Applications to access or amend personal information can be made by completing an Application Form at rti.qld.gov.au or by contacting the Right to Information (**RTI**) and Privacy Group at RTIQCS@corrections.qld.gov.au.

Transferring personal information overseas

QCS can only disclose personal information to an entity outside of Australia when:

- the individual has agreed to the transfer; or
- the disclosure is authorised or required by law; or
- QCS determines there are reasonable grounds to believe that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety, or welfare of an individual, or public health, safety, and welfare; or
- two or more of the following apply:

[9] Accessing and amending personal information before 1 July 2025 was made under the IP Act.

- the recipient is subject to binding privacy obligations that are substantially like the QPPs;
- the disclosure is necessary for QCS to perform its functions;
- the disclosure is for the individual's benefit and it is not possible to seek consent, however if sought it would likely to be given;
- QCS has taken reasonable steps to ensure the information is protected.

Contracted service providers

Under the IP Act, QCS must take all reasonable steps when entering into a service agreement with a contracted service provider (**CSP**) to bind the CSP to the IP Act in relation to the CSP's management of personal information as if it were QCS. Namely:

- a bound CSP must comply with parts 1 and 2 and section 41 of chapter 2 of the IP Act in relation to the QPPs; and
- a bound CSP's compliance with the QPPs may be enforced as if it were QCS; and
- the above requirements continue to apply to the bound CSP in relation to personal information it continues to hold after its obligations under the service agreement otherwise end.

Where a CSP subcontracts with a different organisation, and that organisation comes into possession of QCS' data, the same requirements apply for the subcontracted organisation.

Where it is necessary for personal information to be transferred to a third-party provider to enable that third party to provide services to clients or to QCS, QCS develops and executes contract terms that prevent third party providers from unauthorised use or disclosure of personal information.

Data breaches

A ***data breach*** is defined in the IP Act as:[10]

> *data breach, of an agency, means either of the following in relation to information held by the agency—*
> *(a) unauthorised access to, or unauthorised disclosure of, the information;*
> *(b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur*

QCS is required to assess data breach incidents to understand if it is required to comply with the obligations imposed by the Mandatory Notification of Data Breach (**MNDB**) scheme.[11]

Should a data breach occur, QCS must take reasonable steps to immediately contain and mitigate harm caused by the data breach and commence an assessment to establish the type of data breach that has occurred. The assessment will determine if the incident is a data breach or an ***eligible data breach.***

[10] Schedule 5 IP Act.
[11] Chapter 3A IP Act.

An *eligible data breach*[12] is a data breach that occurs in relation to personal information held by QCS, and **both** of the following apply:

- there is unauthorised access to, or unauthorised disclosure of, personal information held by QCS, or there is a loss of personal information held by QCS in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, **and**
- the unauthorised access to, loss, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual').

As QCS assesses the data breach incident, a data breach may change to a suspected eligible data breach or it may be confirmed that an eligible data breach has occurred. In the case of an *eligible data breach*, QCS has obligations under the MNDB scheme to notify affected individuals and report the breach to the Office of the Information Commissioner (**OIC**).

For more information refer to QCS' Data Breach Policy.

QCS' response to data breaches

QCS requires all data breaches, suspected or otherwise to be promptly notified by all employees and contracted service parties to QCS' Right to Information and Privacy Group and, where the data breach is deemed to be the result of a suspected or confirmed cyber security incident, the QCS Cyber Security Unit at cybersecurity@corrections.qld.gov.au.

Where the QCS Right to Information and Privacy Group is notified of a data breach, it will provide advice and guidance to the relevant business unit where the breach occurred to enable the business unit to take steps (where possible) to immediately contain the breach. Ongoing advice and guidance are also provided during the assessment of the data breach.

If there are reasonable grounds to suspect an eligible data breach has occurred, QCS has 30 days to complete an assessment of the incident and determine if there is a requirement to carry out the notification requirements to affected individuals and the OIC.

If an individual is notified by QCS of an ***eligible data breach***, they will be provided details of a contact person/s. In the first instance, they should continue to contact this person. If they are experiencing issues, they can contact the QCS Right to Information and Privacy Group via email.

Privacy complaints

If an individual believes QCS has breached their privacy in the way their personal information was collected, used, handled, or disclosed, they can make a privacy complaint to QCS.

A privacy complaint must:

- be in writing; and
- provide a contact address; and

[12] Section 47 IP Act.

- give details of the complaint.

It will be investigated in accordance with QCS' Privacy Complaints Policy. Complaints can be emailed or posted to:

Email: privacy@corrections.qld.gov.au
Post: Right to Information and Privacy Group
Queensland Corrective Services
GPO Box 1054, Brisbane QLD 4001

A privacy complaint can also be made via the Queensland Government website at complaints.services.qld.gov.au.

If an eligible privacy complaint is made to QCS within 12 months after the affected individual becomes aware of the breach, or a longer period agreed to by QCS, QCS will respond to the complaint within 45 business days or an agreed response period.

QCS may consider privacy complaints made after 12 months if satisfied the extension is reasonable in the circumstances.

Further information

For further information please contact the QCS Right to Information and Privacy Group:

Email: privacy@corrections.qld.gov.au
Post: Right to Information and Privacy Group
Queensland Corrective Services
GPO Box 1054, Brisbane QLD 4001

Document information and review

Security classification:	Official	Review frequency:	Three (3) years*

*An administrative review of this document will be conducted every three years, or at times of critical content changes.

Current version:	Effective date:	Notes:	Next review due:
1	1 July 2025		1 July 2028