Department of the Premier and Cabinet Privacy Policy

Last updated: June 2025

1. Policy Statement

The Department of the Premier and Cabinet (DPC) is committed to being transparent and accountable in the way we handle personal information. This Privacy Policy demonstrates our commitment to putting systems and processes in place to protect personal information collected, held, used and disclosed in delivering the DPC's services.

2. Scope

This policy applies to all DPC employees in the performance of their duties and explains:

- why we collect personal information;
- how we store information; and
- how we will use and disclose the information.

It has been developed in accordance with Queensland Privacy Principle 1 (QPP1) which requires agencies to have a clearly expressed and up-to-date policy about its management of personal information.

Definitions of key terms are given at the end of this document in section 9.

3. Principles

We are committed to handling personal information lawfully and in a way that responds to privacy expectations of our employees, government stakeholders and communities that we serve. As such, DPC is guided by the following principles:

- Privacy is everyone's responsibility when handling personal information.
- We build privacy into new projects and initiatives from the start.
- We keep personal information safe through robust physical, technical and administrative security controls.
- We measure – and seek to continually improve – our ability to comply with privacy requirements by conducting regular reviews and audits.

4. Responsibilities

At DPC, privacy is everyone's responsibility. All employees receive privacy training to ensure DPC follows the requirements of the Queensland Privacy Principles (QPPs) contained in the *Information Privacy Act 2009* (IP Act). We have a range of practices, procedures and systems in place to meet the requirements under the IP Act.

To foster a strong privacy culture at DPC, we have a Privacy Champion (Associate Director-General, Governance and Engagement) who is responsible for strategic privacy considerations and a Privacy Contact Officer to manage operational privacy activities.

5. Our personal information handling practices

5.1 Kinds of personal information we collect and hold

The definition of 'personal information' is set out in section 9 'Definitions'. We collect and hold personal information to support our business and service delivery functions and employment activities. This information may include:

- personal identification information, including images of people
- electronic signatures
- contact details
- employee records (including employment and education history)
- criminal history checks
- declarations of interest, conflicts of interest and management plans
- personal histories, including health, family, residency status and other legal information
- diversity information
- banking and remuneration details
- consultant/contractor/supplier information
- grant information
- motor vehicle details, including registration.

5.2 How we collect personal information

We collect personal information about individuals and receive personal information from individuals without directly asking for it. Personal information may be collected or received by email, letter, phone contact, forms, surveys, websites administered by DPC, including when an enquiry or submission is made, a DPC event is attended or an application is made for a job with us.

Where possible, we collect the information directly from the person or their authorised representative. Sometimes we collect personal information from a third party but only if:

- we have consent
- we are required or authorised to collect the information from a third party by an Australian law
- it is impracticable or unreasonable for us to collect the information directly from the person.

When we collect personal information, we will take reasonable steps to give a privacy collection notice which explains who we are, why we are collecting the information and who we may disclose it to.

Sometimes we collect sensitive information. The definition of 'sensitive information' is set out in section 9 'Definitions'. Sensitive information is a subset of personal information which accrues some higher protections under the IP Act. Sensitive information can include racial or ethnic origin, membership of a political association, membership of a trade union or professional association, criminal record, health information and other sensitive categories of information. We only collect sensitive information with consent or if we are permitted to collect it by a provision contained in the IP Act.

We take reasonable steps to ensure individuals providing unsolicited personal information understand how the information may be used or disclosed, including by publishing this Policy and including a privacy statement in automatically generated responses to emails and on our website.

5.3 Why we collect personal information

The IP Act requires that we only collect personal information for purposes that are reasonably necessary for, or directly related to, one or more of our functions or activities. At DPC, our core functions and activities involve helping guide government decisions about important policy issues and working closely with other agencies to push forward the government's strategies and plans. There is more information about what we do on the DPC website - About Us.

We collect, hold, use and disclose personal information for a range of purposes related to our functions and activities, including to:

- Undertake consultation on policy, programs and services the Government delivers
- Facilitate events and official visits
- Respond to correspondence
- Respond to right to information requests
- Respond to complaints, including privacy complaints
- Consider sponsorship applications
- Administer awards programs
- Provide administrative and secretariat support to the Queensland Veterans' Council, Queensland Plan Ambassadors' Council, the Queensland Independent Remuneration Tribunal and Domestic and Family Violence Prevention Council
- Undertake recruitment and manage employment matters
- Support Cabinet and Executive Council
- Support appointments to Queensland Government bodies
- Administer legislation within the portfolio responsibilities of the Premier and the Minister for Veterans outlined in the Administrative Arrangements Order available on the Queensland Government website.

Individuals also have the right to interact with us anonymously or using a pseudonym where this is practicable considering the reason for the interaction.

5.4 How we safeguard personal information

We take a range of steps to ensure the personal information we hold is protected against unauthorised access or disclosure and against loss. This includes:

- Technical and IT related security measures (e.g. network security, encryption, incident detection and monitoring, multi-factor authentication)
- Physical security measures (e.g. access-controlled office premises, locked cabinets)
- Role-based access controls (i.e. appropriate user controls are applied)
- De-identification and secure information disposal (where permitted under the *Public Records Act 2023*)
- Procedural measures (e.g. internal policies and procedures governing information security and training for employees, including our Information Security Framework, Privacy Framework and Incident Response Handbook)
- Governance measures (e.g. internal monitoring and audit of security arrangements)
- External standards (e.g. compliance with relevant security standards and regular testing against standards to check compliance).

In addition, we have a Data Breach Policy which sets out our approach to identifying, containing and resolving a data breach, in line with requirements contained in the IP Act.

5.5 Use and disclosure of personal information

DPC endeavours to use and disclose personal information for the purpose for which it was collected and not for another purpose (a secondary purpose) unless we have consent to do so, or otherwise as permitted under the IP Act. For example, the use or disclosure is required or authorised by or under Australian law, there is a serious threat to life, health or safety and it is not possible to get consent.

DPC systems and servers are hosted in Australia. At times, we use other platforms to communicate with the public about our activities and engage with individuals. These include Facebook, X (formerly Twitter), YouTube, LinkedIn, and Instagram. When individuals engage with us in this way, their personal information may be stored by those platforms in countries outside Australia and will be subject to the platform's own privacy arrangements and laws in the platform's jurisdiction.

Generally, DPC does not otherwise disclose personal information to entities outside Australia unless we have sought consent first or an Australian law requires us to disclose the information.

6. Access to and correction of personal information

Individuals have a right to access, and request correction of, personal information we hold about them. This right is set out in QPPs 12 and 13 and in the *Right to Information Act 2009* (RTI Act).

Generally, DPC endeavours to provide individuals with access to their own personal information informally. This may be achieved through current departmental employees exercising their right of access under the *Public Sector Regulation 2023* or by members of the public making a request for access to information under the department's Administrative Access Corporate Policy.

In instances where informal access is not feasible (for example if third parties' personal information is involved), a formal application will be required. These applications do not have a prescribed application form, however a template application form is available on the DPC Right to Information website. The applicant must provide proof of identify before access to personal information can be given.

A person can request access to their personal information, or seek correction of the information, by sending their request to:

privacy@premiers.qld.gov.au or

Manager, Right to Information and Privacy
Department of the Premier and Cabinet
PO Box 15185
CITY EAST QLD 4002

7. Making a privacy complaint

If an individual believes we misused their personal information or did not follow the requirements of the IP Act, they can make a privacy complaint to us. A privacy complaint can also be made on behalf of someone else (such as a child or someone for whom there is written or legal authority to represent).

A privacy complaint must:

- be in writing
- include contact details so we can make contact about the complaint
- provide a description of the privacy issue or concern
- be made within 12 months of becoming aware of the privacy issue.

A privacy complaint can be made online or otherwise in writing in accordance with the DPC Customer Complaint Management Policy. The complaint will be investigated and a written response advising the outcome of the complaint, including any remedies, will be provided within 45 business days.

A person who is dissatisfied with our response may make a privacy complaint to the Office of the Information Commissioner (OIC). A guide outlining the OIC's privacy complaint process is available on the OIC website.

8. Legislation and/or associated documents

8.1 Legislation

Information Privacy Act 2009

Right to Information Act 2009

8.2 Related policies and frameworks

- Data Breach Policy
- DPC Customer Complaints Management Policy

8.3 Publication scheme

The DPC Publication Scheme is available online.

9. Definitions

Word or term	Definition
Personal information	is defined in section 12 of the IP Act and *means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:* *a) whether the information or opinion is true or not; and* *b) whether the information or opinion is recorded in a material form or not."* Examples of personal information include a person's name, address, date of birth or telephone number. An individual does not need to be directly identified in the information for it to be personal information. It is sufficient if an individual can be reasonably identified by reference to other information.
Sensitive information	is defined in schedule 5 of the IP Act and *means:* *(a) information or an opinion, that is also personal information, about the individual's—* *(i) racial or ethnic origin; or* *(ii) political opinions; or* *(iii) membership of a political association; or* *(iv) religious beliefs or affiliations; or* *(v) philosophical beliefs; or* *(vi) membership of a professional or trade association; or* *(vii) membership of a trade union; or* *(viii) sexual orientation or practices; or* *(ix) criminal record;* *(b) health information about the individual;* *(c) genetic information about the individual that is not otherwise health information;* *(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or* *(e) biometric templates.*

Word or term	Definition
	Sensitive information is a subset of personal information which accrues some higher protections under the IP Act.