Office of the Inspector-General of Emergency Management

Privacy Policy

Version 1.0
Date: July 2025

Contents

Introduction

The Office of the Inspector-General of Emergency Management (the Office) 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 Office services.

Scope

The Office's Privacy Policy applies to all employees in the performance of their duties and explains:

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

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

Principles

The Office is 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. To achieve this, the Office is guided by the **QPPs** in the *Information Privacy Act 2009* (Qld) (**IP Act**) which set out the rules for how agencies deal with personal information.

The Office privacy practices include:

- privacy is everyone's responsibility when handling personal information
- personal information is kept safe through technical and administrative security controls
- we only collect personal information that we need for our functions and activities
- we give individuals information about why we collect their personal information and how we will use it.

The Office personal information handling practices

Section 12 of the IP Act defines personal information as:

'Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:

- whether the information or opinion is true or not
- whether the information or opinion is recorded in a material form or not.

Kinds of personal information the Office collects and holds

The Office collects and holds 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.

Why the Office collects personal information

The IP Act requires that the Office only collect personal information for purposes that are reasonably necessary for, or directly related to, one or more of our functions or activities. The Office collects, holds, uses, and discloses personal information for a range of purposes related to our functions and activities, including to:

- undertake consultation on policy, reports, 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
- undertake recruitment and manage employment matters.

How IGEM collects personal information

Personal information may be collected by email, letter, phone, forms, surveys, websites administered by the Office, or by noting information provided verbally.

Where possible, the Office collects information directly from the person or their authorised representative.

Sometimes the Office may collect sensitive information, when we reasonably believe that the information is necessary for, or directly related to, an Office function or activity.

The definition of 'sensitive information' is set out in the IP Act (s9). Sensitive information is a subset of personal information which has 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. The Office only collects sensitive information with consent and if the information is reasonably necessary for or directly related to one or more of the Office's functions, unless an exception applies.

Personal information can be stored in a variety of ways such as on paper, electronic database, photographic and video images, audiotape and/or digital format.

Notification of the collection of personal information

. When collecting personal information, the Office must take reasonable steps to inform individuals about:

- the purpose of collection and how the information will be used
- any legal authority for the collection
- to whom the information may be disclosed.

How the Office safeguards personal information

The Office takes 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)
- where permitted by the *Public Records Act 2023* (Qld), the Office will destroy or deidentify unsolicited personal information or personal information no longer required for any of its functions in accordance with our obligations under the QPPs if it is lawful and reasonable to do so
- procedural measures
- ensuring there is a Data Breach Policy in place, which sets out the Office's approach to identifying, containing, and resolving a data breach, in line with requirements contained in the IP Act. Chapter 3A of the IP Act creates a mandatory notification of data breach (MNDB) scheme.

Use and disclosure of personal information

The Office 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. This may include:

- managing associated administrative processes including recruitment and human resources administration and staff management functions
- submission data used for assurance work including preparing reports.

At times, the Office may use other platforms to communicate with the public about our activities and engage with individuals. These may include, but not limited to, social media platforms or surveys. 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. By choosing to interact with us via these platforms, individuals consent to the disclosure of their personal information outside Australia and acknowledge that it may not be protected under the *Australian Privacy Act 1988*. Generally, the Office 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.

Where the Office does disclose personal information, this will only occur either by gaining the individuals consent, where the Office is authorised or required by to law or otherwise consistent with our obligations under the IP Act.

Access to and correction of personal information

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

Generally, the Office endeavours to provide individuals with access to their own personal information when requested. This may be achieved through current 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.

In instances where direct access is not feasible (for example if third parties' personal information is involved), a formal request is required. To make a formal request, the applicant must submit a Right to Information (RTI) application through the Queensland Government's online portal: Information Access application | Right to Information and Information Privacy

Making a privacy complaint

If an individual believes the Office misused their personal information or did not follow our obligations under the IP Act, they can lodge a privacy complaint. 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 made **in writing and include the following**:

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

Making a privacy complaint to the Office of the IGEM

Send an email to the Principal Executive Officer at: IGEM.corro@igem.qld.gov.au

Time frame for handling a privacy complaint

Under the IP Act, the Office must provide a response to a complaint within 45 (business or just flat) days of receipt of the complaint.

If you are not satisfied with the outcome of your complaint, you can refer your privacy complaint to the Office of the Information Commissioner via: email: administration@OIC.qld.gov.au.

Appendix A – Related Policy documents and supporting documents

Legislation

- *Public Sector Act 2022*
- *Public Records Act 2023*
- *Right to Information Act 2009*
- *Information Privacy Act 2009* (Schedule 3 contains the Queensland Privacy Principles which are a set of rules that regulate how Queensland government agencies handle personal information)

Policy

- Data Breach Policy
- Data Breach Register

Appendix B – Key Definitions

Mandatory Notification of Data Breach (MNDB)	Mandatory Notification of Data Breach scheme is contained in Chapter 3A of the IP Act. It imposes obligations on agencies to prepare, respond and communicate in the event of suspected eligible data breaches or confirmed eligible data breaches. The MNDB scheme commenced on 1 July 2025 for Queensland government agencies.
Personal Information	Section 12 of the IP Act provides that personal information means information or an opinion about an identified living individual or a living individual who is reasonably identifiable, whether it is true or recorded in a material form. The individual does not need to be directly identified in the information for it to be personal information. It is sufficient if they can reasonably be identified reference to other information. Information does not have to be true in order to be personal information and it does not need to be written down or recorded in a material form, such as a photograph or audio recording.
Queensland Privacy Principles (QPP)	The Queensland Privacy Principles in the *Information Privacy Act 2009* set the rules for how agencies deal with personal information.
Sensitive Information	Sensitive information is: • information or an opinion, that is also personal information, about the individual's - racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of professional or trade association, membership of a trade union, sexual orientation or practices and criminal record. • health information about the individual • genetic information about the individual that is not otherwise health information • biometric information that is to be used for the purpose of automated biometric verification or biometric identification or biometric templates.
Unsolicited personal Information	Unsolicited personal information is personal information received by an agency that the agency took no active steps to collect. It is information that someone gives or sends to an agency at their own instigation, for example a petition from a community member that includes their personal information and the personal information of the signers.