Submission template - 2025 disaster events reviews

Please complete the sections below and email your submission to info.igemreviews@igem.qld.gov.au.

1. Submitter details

Details			
Submission title	Disaster Events: Access to Information, Privacy Principles and Information Sharing		
Organisation	Office of the Information Commissioner		
Contact name	Sarah Owens	**Position:**	A/Manager, Policy
Email	policy@oic.qld.gov.au	**Phone**	07 3234 7392

2. Which review(s) does your submission relate to?

☐ North Queensland Floods (late January to early February 2025)

☐ Tropical Cyclone Alfred – South-East Queensland (late February to early March 2025)

☐ Western Queensland Floods (late March to early April 2025).

3. Supporting documentation

☐ I will email additional documentation to support my submission (e.g. reports, case studies, photos).

4. Confidentiality

Thank you for taking the time to provide evidence. Permission will be sought where specific information is to be quoted, or photos or diagrams are to be attributed.

Please indicate your preference below:

☒ I consent to my submission being published in full.

☐ I consent to my submission being published in summary form only.

☐ I do not consent to my submission being published.

Instructions:

- Use the prompts below to guide your submission. Delete as needed.
- Submit by sending this completed template to: info.igemreview@igem.qld.gov.au
- You may wish to attach photos or diagrams to the email with your submission.
- Submissions close: Monday, 7 July 2025.

1. Pre-season preparedness and planning activities undertaken in the 12 months leading up to the event/s is of interest.

Prompts to guide your submission (can be deleted):

- Information and data sharing protocols in place; how protocols supported pre-season preparedness and understanding of vulnerabilities

Submission

The Office of the Information Commissioner (**OIC**) welcomes the opportunity to make a submission to the Office of the Inspector-General in relation to its review into the 2025 disaster events.

As OIC is not directly involved in disaster management, this submission is confined to access to information, privacy principles and information sharing, noting this aligns with outcome 7 in the Standard for Disaster Management in Queensland.

About the OIC

OIC is an independent statutory body that reports to the Queensland Parliament. The Information Commissioner is an Officer of Parliament and is charged with functions under the *Right to Information Act 2009* (**RTI Act**) and the *Information Privacy Act 2009* (**IP Act**).

On 1 July 2025, the main provisions of the *Information Privacy and Other Legislation Amendment Act 2023* commenced, with significant changes to the RTI and IP Act including:

- simplified application process to access information and amend personal information, with all applications now made under the RTI Act
- replacement of the Information Privacy Principles and National Privacy Principles with the Queensland Privacy Principles
- updated definitions of personal information and sensitive information, and
- Mandatory Notification of Data Breach scheme for Queensland public sector agencies (delayed for local government).

Right to Information Act

Overview

The RTI Act promotes openness, accountability and transparency by facilitating greater access to government-held information.

Access to information

The RTI Act supports the administrative release of government-held information as a matter of course (unless there is a good reason not to) for example, through an agency's website, publication scheme, disclosure log, open data portal or administrative access scheme. Formal applications for government-held information (personal and non-personal) under the RTI Act should only be made as a last resort.

It is noted that the management of the 2025 disaster events involved a proactive approach to the timely publication of important information prior and during the events. However, the impacts of these events have far-reaching and long-term impacts on affected members of the community, who may seek access to very specific information about their property, personal rights or health and how decisions on disaster management may have affected those. Accordingly, it is important that all agencies involved in disaster

management have a clearly agreed approach to how such information is documented, retained and made available when requested.

Transparency by design

OIC recommends that Queensland public sector agencies adopt a 'transparency by design' approach to service delivery, decision-making and disclosure of information.

It is noted that various public sector agencies have shared responsibilities under the Standard for Disaster Management in Queensland. Those shared responsibilities focus on effective outcomes in managing disasters under the Emergency Management Assurance Framework and depend on decisions being made in highly volatile and fast-moving circumstances.

In such an environment, it is important that all agencies adopt a 'transparency by design' approach – meaning they ensure that all decisions and key information sets influencing those decisions are documented and made available to the community as soon as possible. This meets the pro-disclosure bias advanced under the RTI and IP Act and requires agencies to leverage their existing mechanisms, like administrative access schemes and publication schemes, to ensure that information is published or made available on request.

Information Privacy Act

Overview

The IP Act provides for the fair collection and handling of personal information by Queensland public sector agencies. The IP Act includes the Queensland Privacy Principles (QPPs) which regulate the collection, management, use and disclosure of personal information, and the Mandatory Notification of Data Breach scheme.

The IP Act applies to Queensland public sector agencies including the Queensland Police Service, Queensland Fire Department, Department of Local Government, Water and Volunteers, local governments and State, district and local disaster management groups.

The IP Act is intended to operate subject to the provisions of other Acts regulating the collection, storage, handling, accessing, amendment, management, transfer, use and disclosure of personal information.

Queensland Privacy Principles

From 1 July 2025, all Queensland public sector agencies must comply with the QPPs when managing personal information. Personal information is any information about an identified individual or who is reasonably identifiable from the information. If an agency wishes to share information which is not personal information, then the QPPs do not apply.

It is a common misconception that the privacy principles in the IP Act work against the sharing of information between agencies. The privacy principles not only provide generous flexibility for information sharing in disaster events but do so without compromising the privacy of that information once the disaster event has been dealt with.

While the IP Act includes generous flexibilities which an agency can rely on in the event of a disaster, agencies must still deal fairly with personal information. Personal information can only be collected if it is reasonably necessary for, or directly related to, an agency's functions or activities.

The QPPs of particular relevance to disaster events are summarised below.

Collection notices

QPP 5 provides that an agency collecting personal information about an individual must take steps that are reasonable in the circumstances to:

- notify the individual of the matters mentioned in QPP 5.2 that are reasonable in the circumstances, or

- otherwise ensure that the individual is aware of those matters.

In the context of a disaster event, there may be no or few reasonable steps the agency can take to notify an individual about the collection of their personal information, and many of the QPP 5.2 matters may not be relevant.

Collection, use or disclosure of personal information

QPP 3 provides that an agency must not collect personal information, other than sensitive information, unless the information is reasonably necessary for, or directly related to, one or more of the agency's key functions. It also provides that an agency must not collect sensitive information about an individual unless:

- the individual consents to the collection of the information and the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities.
- QPP 3.4 applies in relation to the information.

QPP 6 provides that if an agency holds personal information about an individual that was collected for a particular purpose (primary purpose), the agency must not use or disclose the information for another purpose (secondary purpose) unless:

- the individual consents to the use or disclosure of the information.
- QPP 6.2 applies in relation to the use or disclosure of the information.

Under QPP 3.4, an agency can collect information without consent, and under QPP 6.2(c) an agency can use or disclose personal information for a secondary purpose, if a permitted general situation applies. The permitted general situations are listed in schedule 4, part 1 of the IP Act. Permitted general situations, of relevance to disaster events, appear below.

Threats to life, health and safety

A permitted general situation can exist if both of the following apply:

- it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and
- the agency reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety.

The nature of disaster events will often make obtaining consent impracticable. While it could appear limiting that the threat must be serious, Queensland's experience has shown that disaster events often have tragic consequences, meaning they will generally represent a serious threat. It is not necessary for the threat to be immediate or imminent, encompassing steps taken to ensure the threat does not eventuate.

Missing persons

A permitted general situation can exist if both of the following apply:

- the agency reasonably believes that the collection, use or disclosure is reasonably necessary to assist an entity to locate a person who has been reported as missing, and
- the collection, use or disclosure complies with a guideline* in effect under chapter 3, part 2.

A permitted general situation could arise in relation to a missing person during a disaster event where information sharing is reasonably necessary to assist with locating the person. *Note: the guideline has not commenced at the time of writing however there will generally be other QPPs that an agency can rely on to collect, use or disclose personal information in these circumstances.

Integrity of personal information

A critical component of coordinated responses to disaster events is the sharing of information, including the personal information of individuals affected by such events.

Agencies must take reasonable steps to ensure the quality of the personal information collected, used or disclosed (QPP 10). In addition, agencies holding personal information must take reasonable steps to protect the information from misuse, interference, loss, unauthorised access modification or disclosure (QPP 11).

Information sharing between agencies

Agencies should prepare for sharing information in response to disaster events. An *Information Sharing Strategy* may be useful to assist with anticipating situations that may require the sharing of personal information and ensuring appropriate arrangements are in place.

Any personal information sharing arrangement should identify the purpose of the information sharing, whether the sharing is authorised by an Act, and whether disclosure is compliant with the QPPs.

Agencies may also wish to consider undertaking a *Privacy Impact Assessment* (PIA) to identify, assess and manage any risks associated with information sharing. Even if a PIA is not developed, assessing the risks can be an important part of privacy compliance.

Consideration may be given to sharing aggregated or de-identified data where the identity of individuals is not needed, for example, the evacuation centre has two people with diabetes and 3 pregnant people. This approach is less likely to raise privacy concerns.

Agencies could also consider whether consent to use or disclose personal information could be obtained in advance of a disaster event, with the consent to be relied on should a disaster occur.

OIC has published guidelines on information sharing in disaster events including:

- Information sharing: generally, for law enforcement, and in disaster events
- Privacy flexibility in disaster management - information sharing scenarios

We trust this submission will assist with your review. Please advise if you require further information.

2. Response operations – if your submission refers to more than one event please specify the relevant event in the information below.

Prompts to guide your submission (can be deleted):

- Effectiveness of business continuity plans (BCPs) activated including BCPs of other entities
- Collaboration and coordination within your entity and across other agencies
- Collaboration and coordination involving community groups or leaders
- Examples of agencies collaboration to support capability and sustain capacity during response
- Examples of resource sharing and prioritisation within and across disaster management groups or other entities
- Arrangements such as MOUs and how these supported response
- Examples of decisions informed by intelligence and the impacts the decisions made to community outcomes
- Information and data sharing arrangements which supported response activities
- Effectiveness of information and data sharing to inform response activities
- Examples of identified interdependencies and collaborative problem solving with other entities
- Examples of operations which improve the community's ability to cope with future events
- Good practice examples that involved integration of response activities
- Opportunities for improvement involving integration of response activities

3. Opportunities to enhance community resilience to better prepare for and respond to future disasters.

Prompts to guide your submission (can be deleted):

- Examples of your regional resilience strategies which helped the community better prepare for the event/s
- How your resilience strategies enabled the community to better respond to the event/s
- Community organisation or leader involvement in the development of resilience strategies
- Any initiatives or arrangements for critical infrastructure redundancies that support community connectedness during disasters (e.g. electricity, telecommunication)
- Examples of volunteer management to support community resilience
- Evaluation of resilience initiatives and programs including lessons identified
- Integration of resilience priorities in disaster management plans and supporting doctrine for preparedness and response
- Good practice examples of enhanced community resilience during response
- Collaboration and coordination with other entities to strengthen community resilience

Once you have completed this form, please email to info.igemreview@igem.qld.gov.au

Thank you for your contribution. Your feedback will help strengthen Queensland's disaster preparedness and response.