Data Breach Policy

1. Purpose and scope

This Data Breach Policy (**the policy**) establishes the framework for identifying, managing and responding to data breaches within the Department of Families, Seniors, Disability Services and Child Safety (**the department**).

It is developed in compliance with the *Information Privacy Act 2009* (**IP Act**), the Queensland Government Information and Cyber Security Policy (**IS18:2025**), and other relevant legislation.

The policy aims to protect the privacy of individuals, safeguard information held by the department and minimise harm arising from data breaches.

Effective breach management, including notification as appropriate, helps the department to avoid or reduce harm to affected individuals. It also provides an opportunity to learn from incidents and strengthen data protection measures.

This policy applies to all employees, contractors, subcontractors, consultants, third-party service providers, and volunteers who handle departmental data, including personal information, sensitive information and confidential data. It covers all data breaches, whether accidental or deliberate, that occur within the department's IT systems, physical records or third-party services.

2. Policy statement: Responding to a Data Breach

2.1 Reporting a Data Breach

2.1.1 Internal reporting

All actual or suspected data breaches that affect personal information must be reported immediately to the department's Information Privacy and Governance team.

Where the data breach is also an information security incident, the data breach must also be reported to the Service Desk or the Information Security team.

2.1.2 External reporting

Members of the public can report a suspected data breach by contacting the department through its website or by phone.

2.2 Responding to a Data Breach

The department will follow a six-stage process to respond to data breaches:

2.2.1 Stage 1: Preparation

- Maintain an up-to-date Data Breach Response Plan.
- Conduct regular training for employees on data breach prevention and response.
- Ensure robust security measures are in place, including encryption, access controls, and regular audits.

2.2.2 Stage 2: Identification

- Identify and report suspected data breaches immediately to the department's Information Privacy and Governance team. Information security incidents must also be referred to the Service Desk or the Information Security team,
- Conduct an initial assessment to determine whether a data breach has occurred.
- Document the details of the incident, including the date, time, and nature of the breach.

2.2.3 Stage 3: Containment and mitigation

- Take immediate steps to contain the breach and prevent further unauthorised access or disclosure.
- Implement measures to mitigate harm.

2.2.4 Stage 4: Assessment

- Assess the scope and impact of the breach, including:
  - the type of data involved
  - the number of individuals affected, and
  - the potential for serious harm.
- Determine whether the breach meets the criteria for an **eligible data breach** under the IP Act and the Mandatory Data Breach Notification (**MDBN**) scheme.

2.2.5 Stage 5: Notification

- If the breach is deemed to be an eligible data breach, notify the Office of the Information Commissioner Queensland (**OIC**) and affected individuals as soon as practicable.
- Notifications must include:
  - a description of the breach
  - the type of information involved
  - steps individuals can take to protect themselves
  - contact details for further information, and
  - if notification is not required, document the reasons for this decision.

2.2.6 Stage 6: Post data breach review and remediation

- Conduct a post-incident review to identify the root cause of the breach and evaluate the effectiveness of the response.
- Implement corrective actions to prevent future breaches, such as updating policies, improving security measures, or providing additional training.

3. Register of eligible data breaches

The department will maintain an internal Register of Eligible Data Breaches, which will include:

- details of the breach (eg date, nature and scope)

- actions taken to contain and mitigate the breach
- assessment outcomes and notification decisions, and
- post-incident review findings and remediation actions.

The department will review and update the Register on a regular basis.

4. Recordkeeping

The department will document its management of, and response to, actual or suspected data breaches, in accordance with the *Public Records Act 2023.* Records will include evidence of compliance with this policy and relevant legislation.

5. Related legislation and policies

The department manages data breaches in accordance with:

- Legislation and standards:
  - *Information Privacy Act 2009* (Qld)
  - *Public Sector Act 2022* (Qld)
  - *Human Rights Act 2019* (Qld)
  - Queensland Government Information and Cyber Security Policy (IS18:2025)
  - Cybersecurity laws and regulations applicable to Queensland Government agencies

- Policy:
  - Department of Families, Seniors, Disability Services and Child Safety Privacy Policy
  - Information Security Incident Response Plan
  - Data Breach Response Plan
  - Acceptable Use Policy

6. Roles and responsibilities

Role	Responsibility
Employee	Read the Data Breach Policy and Data Breach Response Plan and understand what is expected of them. Comply with the IP Act, including protecting personal information held by the department from unauthorised access, disclosure or loss. Where required in accordance with this Data Breach Policy, immediately report a data breach or suspected data breach to the appropriate officer (this could be a supervisor, manager, senior officer or privacy officer). Respond to requests for information from and cooperate with the Privacy Officer and/or the Data Breach Response Team. Comply with record keeping obligations.
Manager, Information Privacy and Governance	Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates.

Role	Responsibility
	Escalate serious data breaches to relevant senior officer or executive. Notify (or arrange for a senior officer or executive to notify) the Information Commissioner, affected persons and others where required. This includes publishing, monitoring and reviewing the currency of public notifications of a data breach published to the agency website under section 53(1)(c) IP Act. Immediately report a data breach that is also a cyber security incident to the Service Desk or Information Security team, if not already reported. Maintain the Register of Eligible Data Breaches. Maintain and update this Policy.
Managers	Identify and escalate concerns within area of responsibility which may enliven the requirements of this Data Breach Policy. Immediately report a data breach that is also a cyber security incident to the Service Desk or Information Security team, if not already reported.
Senior Management	Immediately report a cyber security incident that is also a data breach to the Information Privacy and Governance team, if not already reported. Where relevant, notify the Information Commissioner, affected persons and others where required. Implement the Information Security Incident Response Plan and related procedures if the data breach is also a cyber security incident. Convene the Information Security Incident Response Team, when appropriate
Information Security Incident Response Team [note that members are drawn from various teams within the department]	Manage a data breach that is considered likely to cause serious harm to any impacted individual or the agency's systems.

7. Definitions

Term	Meaning
Affected individual	An “affected individual” under section 47(1)(ii) of the IP Act.
Data breach	The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
Data Breach Policy	This Policy.
Data Breach Response Plan	A more detailed procedural document complementing the Data Breach Policy, which could be an internal document detailing the agency's more specific processes in managing and responding to a data breach.

Term	Meaning
Eligible Data Breach	An "Eligible Data Breach" will have occurred under section 47 of the IP Act where: (a) there has been unauthorised access to, or unauthorised disclosure of **personal information** held by an agency, **and** the access or disclosure is likely to result in **serious harm** to any of the **individuals** to whom the information relates; **or** (b) there has been loss of **personal information** held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, **and** the loss is likely to result in **serious harm** to any of the **individuals** to whom the information relates.
Employee	A person who carries out work in any capacity for an agency as defined in section 7 of the *Work Health and Safety Act 2011* (Qld), including work as: (a) an employee (b) a contractor or subcontractor or an employee of a contractor or subcontractor (c) an apprentice or trainee (d) a student gaining work experience, or (e) a volunteer.
Information Commissioner	The Queensland Information Commissioner.
IP Act	The *Information Privacy Act 2009* (Qld).
Information security event	An information security 'event' is 'an identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant' [ISO/IEC 27000:2018].
Information security incident	An information security 'incident' is defined as 'a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security' [ISO/IEC 27000:2018]
***Held* or *hold* in relation to personal information**	Personal information is held by a relevant agency, or the agency holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant agency.
Personal information	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.
Serious harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example:

Term	Meaning
	(a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or (b) serious harm to the individual's reputation because of the access or disclosure.

8. Approval and review

Approved by:

Arthur O'Brien

Acting Director-General

10 July 2025

Policy to be reviewed in July 2026.