	COUNCIL POLICY	
	Data Breach	
	Policy Number	CP102
	Directorate	Organisational Services
	Owner	Corporate Services
	Last Approved	22 July 2026
	Review Due	22 July 2030

1. PURPOSE

This policy outlines Council's overall approach to preventing, detecting and responding to data breaches.

2. SCOPE

This policy applies to all Fraser Coast Regional Council Councillors and employees and covers all work-related dealings with each other and with customers, contacts, clients, members of the public, suppliers and any other individuals whose personal information is collected, used or held by Council.

Further, this policy applies to all personal information in any form, including information created, received, stored, accessed or transmitted through Council systems, devices, applications or records, whether electronic or hard copy. It applies to all suspected or actual data breaches, including suspected **Eligible Data Breaches**, regardless of how they occur.

3. HEAD OF POWER

This policy is established under the authority of the *Information Privacy Act 2009* (Qld) (the **IP Act**), including the amendments introduced by the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (**IPOLA**), which require agencies to have a Data Breach Policy outlining how they will identify, assess and respond to data breaches, including Suspected Eligible Data Breaches.

This policy also supports Council's broader obligations to protect personal information and to manage records in accordance with the *Local Government Act 2009* (Qld) (the **LG Act**), the *Public Records Act 2002* (Qld) and any other applicable legislation, regulations or binding guidelines.

4. POLICY STATEMENT

Council is committed to protecting personal information, reducing the risk of harm to individuals, and maintaining community trust in how personal information is managed. Council recognises that a clear and coordinated response to data breaches is essential to ensuring that affected individuals are informed and supported, that risks are minimised, and that Council meets its legislative responsibilities under the IP Act and the IPOLA.

Council will take all reasonable steps to prevent, detect and respond to data breaches. This includes promptly assessing all suspected or actual data breaches, determining whether an Eligible Data Breach has occurred, notifying affected individuals and the OIC when required, and

taking appropriate actions to contain and manage the breach. Council will also review all data breaches to support continuous improvement of its information management practices.

4.1. Roles and responsibilities

Role	Responsibility
Councillors and employees	• Read the Data Breach Policy and Cyber Security Incident Response Plan and understand what is expected of them. • Comply with the IP Act, including protecting personal information held by the agency 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, cyber security officer, or governance officer). • Respond to requests for information from and cooperate with Governance and/or the CSIRT. • Comply with record keeping obligations.
Manager	• 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 Director Organisational Services, if not already reported.
Director Organisational Services & Transformation	• Immediately report a cyber security incident that is also a data breach to Governance, if not already reported. • Where relevant, notify the Information Commissioner, affected persons and others where required. • Implement the Cybersecurity Incident Response Plan and related procedures if the data breach is also a cyber security incident. • Convene the CSIRT, when appropriate
Cyber Security Incident Response Team (CSIRT)	• Manage a data breach that is considered likely to cause serious harm to any impacted individual or the agency's systems.
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. • 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). • Immediately report a data breach that is also a cyber security incident to the Director Organisational Services & Transformation, if not already reported. • Maintain the Register of Eligible Data Breaches. • Maintain and update this Policy.

4.2. Responding to a Data Breach

4.2.1. Stage 1: Preparation

Council will maintain clear governance arrangements, training, systems and processes to support the early identification and effective management of data breaches. Preparation includes ensuring awareness of responsibilities, maintaining incident response capability and promoting good information handling practices.

4.2.2. Stage 2: Detection

Council will act promptly to identify suspected or actual data breaches. All councillors and employees are expected to report any incident or concern that may involve the loss, unauthorised access or unauthorised disclosure of personal information.

4.2.3. Stage 3: Respond

Council will take immediate steps to contain the breach and limit any further unauthorised access, disclosure or loss of personal information. Council will also take reasonable steps to reduce or prevent potential harm to affected individuals.

4.2.4. Stage 4: Assessment

Council will assess all suspected or actual data breaches in a timely manner to determine the nature and extent of the breach, the personal information involved, the potential impacts and whether an Eligible Data Breach has occurred.

4.2.5. Stage 5: Notification

If an Eligible Data Breach is identified, Council will notify affected individuals and the Office of the Information Commissioner in accordance with legislative requirements. Council may also notify individuals for non-eligible breaches where it is appropriate to support transparency or reduce harm.

4.2.6. Stage 6: Recover and Lessons Learnt

Council will review data breaches to understand their causes, identify lessons and implement improvements to prevent recurrence. Council will take steps to strengthen practices, systems or procedures where required.

4.3. Register of Eligible Data Breaches

Council will maintain a Register of Eligible Data Breaches in accordance with the IP Act. The Register will record all Eligible Data Breaches that require notification to affected individuals and the Office of the Information Commissioner. Council will ensure the Register is accurate, secure and updated in a timely manner. The information recorded in the Register will support Council to meet its legislative obligations, monitor trends and strengthen its overall information management practices.

4.4. Councillors and employee conduct matters

Where a suspected or actual data breach involves, or appears to involve, the behaviour of a councillor or employee, Council will manage the data breach response in accordance with this policy. Any related concerns about conduct will be assessed and managed separately under Council's relevant conduct, disciplinary, fraud and corruption, public interest disclosure, complaints management, or other applicable frameworks.

This may include referral to the appropriate internal or external body where required by law or Council policy. The management of any conduct matter does not replace Council's obligations to assess, contain, notify and record the data breach in accordance with this policy.

4.5. Record keeping

Council will create and maintain complete and accurate records of all suspected and actual data breaches, including incident logs, evidence registers, reports, assessments, decisions, notifications and actions taken to manage the breach. Records will be managed in accordance with the *Public Records Act 2002* (Qld), Council's Records Management Policy and any other applicable legislative obligations. Effective record keeping ensures accountability, supports consistent decision-making and enables Council to demonstrate compliance with information privacy requirements.

5. DEFINITIONS

To assist in the interpretation of this Policy, the following definitions apply:

"Agency Worker" means 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.

"Affected individual" means an "affected individual" under section 47(1)(ii) of the IP Act.

"Councillor" means the Mayor and Councillors of Fraser Coast Regional Council.

"Council" means the Fraser Coast Regional Council.

"CSIRT" means the Cyber Security Incident Response Team.

"Cyber Security Incident Response Plan" means a more detailed procedural document complementing the Data Breach Policy, detailing Council's more specific processes in managing and responding to a cyber security incident, including a data breach.

"Data breach" means 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" means this Policy.

"Eligible Data Breach" means 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.

"Employees" means employees of Council, including full-time, part-time, casual or fixed term employees of Council including any volunteers, contractors, consultants and agency workers who perform work for or on behalf of Council.

"IP Act" means the *Information Privacy Act 2009* (Qld).

"Held or hold in relation to personal information" means 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.

"LG Act" means the *Local Government Act 2009* (Qld).

"OIC" means the Office of the Information Commissioner.

"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 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" means to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example:

(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.

6. ASSOCIATED DOCUMENTS

- *Information Privacy Act 2009*
- *Local Government Act 2009*
- *Public Records Act 2002*
- Data Breach Register (eDOCS #5408908)
- Cyber Security Incident Response Plan (eDOCS #5337537)
- Cyber Security Incident Response Plan Data Breach Playbook (eDOCS #5360687)
- CP007 Complaints Management Council Policy (eDOCS #2991947)
- CP014 Fraud and Corruption Control Council Policy (eDOCS #841181)
- CP019 Public Interest Disclosure Management Council Policy (eDOCS #1968369)
- CP099 Information Privacy Council Policy (eDOCS #5303360)
- MP023 Code of Conduct Management Policy (eDOCS #1969232)
- MP026 Discipline Management Policy (eDOCS #804149)

7. REVIEW

This Policy will be reviewed on a risk-based methodology and will be reviewed at least every four years.

Version Control

Version Number	Key Changes	Approval Authority	Approval Date	Document Number
1	New Policy	Council OM	22 July 2026	5408910