CASSOWARY COAST REGIONAL COUNCIL

Data Breach Response Plan

Policy type	Administration
Function	Corporate & Community Services
Policy Owner	Information Communication & Technology
Effective date	23 July 2020
Last review date	19 February 2026

1. Purpose

A data breach occurs when personal information is lost or subjected to unauthorised access or disclosure. For good privacy practice purposes, this response plan also covers any instances of unauthorised use, modification or interference with personal information held by Cassowary Coast Regional Council (Council). Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals and entities.

This response plan is intended to enable Council to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

2. Scope

This plan applies to all Council staff, contractors, volunteers and elected representatives who handle personal information on behalf of Cassowary Coast Regional Council.

3. Definitions

Assessment – Evaluation of the data breach's cause, impact, and notification requirements.

Confidential information – is information generally not, known by or available upon request, to the public which could be specifically referred to as such information that may not relate to Council's commercial or other activities or may include legal advice obtained by Council. Such confidential information includes discussions, documents, electronic data/media, tape recording, emails, facsimiles or attachments.

Containment – actions taken to limit the impact of a data breach.

Eligible Data breach – occurs when personal information is lost, subjected to unauthorised access or disclosure; accidental or unauthorised destruction or alteration or loss of availability of personal information.

IPOLA - *Information Privacy and Other Legislation Amendment Act 2023* (Qld) outlines mandatory data breach notification.

Local Government Employee Individuals employed by Cassowary Coast Regional Council under a formal employment agreement, including full-time, part-time, casual, and temporary staff. For the purposes of this policy, "employees" may also refer to contractors, volunteers, and elected representatives when they are acting in an official capacity on behalf of Council and handling personal information.

Notification – informing affected individuals and authorities about a data breach.

OAIC – means the Office of Australian Information Commissioner.

QPP - *Queensland Privacy Principles under the Information Privacy Act 2009* that govern how personal information must be collected, stored, used, and disclosed by Queensland government agencies.

Personal information – is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Remediation – Steps taken after a data breach to prevent future incidents.

4. Roles and Responsibilities

Chief Executive Officer (CEO)

The CEO oversees all breach responses and approves notifications.

- Provides strategic oversight of all breach responses.
- Approves formal notifications to affected individuals and external bodies, including the Office of the Information Commissioner (OIC).
- Ensures Council's breach response aligns with the *Information Privacy Act 2009* and IPOLA 2023.
- Authorises post-incident reviews and remediation plans.

Governance Team

The Governance Team coordinates breach assessment, containment, and notification.

- Leads breach assessment and notification processes.
- Coordinates internal reporting and documentation of breach incidents.
- Liaises with the OIC for mandatory notifications and compliance queries.
- Maintains and updates the Data Breach Response Plan.
- Oversees privacy training and awareness programs for staff.
- Conducts post-breach reviews and ensures lessons learned are documented and actioned.

Manager ICT

The Manager ICT assists with technical containment and investigation of all breaches.

- Identifies and contains technical aspects of the breach (eg. Compromised systems, unauthorised access).
- Investigates root causes and supports forensic analysis.
- Implements immediate mitigation strategies to prevent further data loss.
- Provides technical input into breach assessments and remediation planning.
- Maintains system logs and evidence for internal and external review.

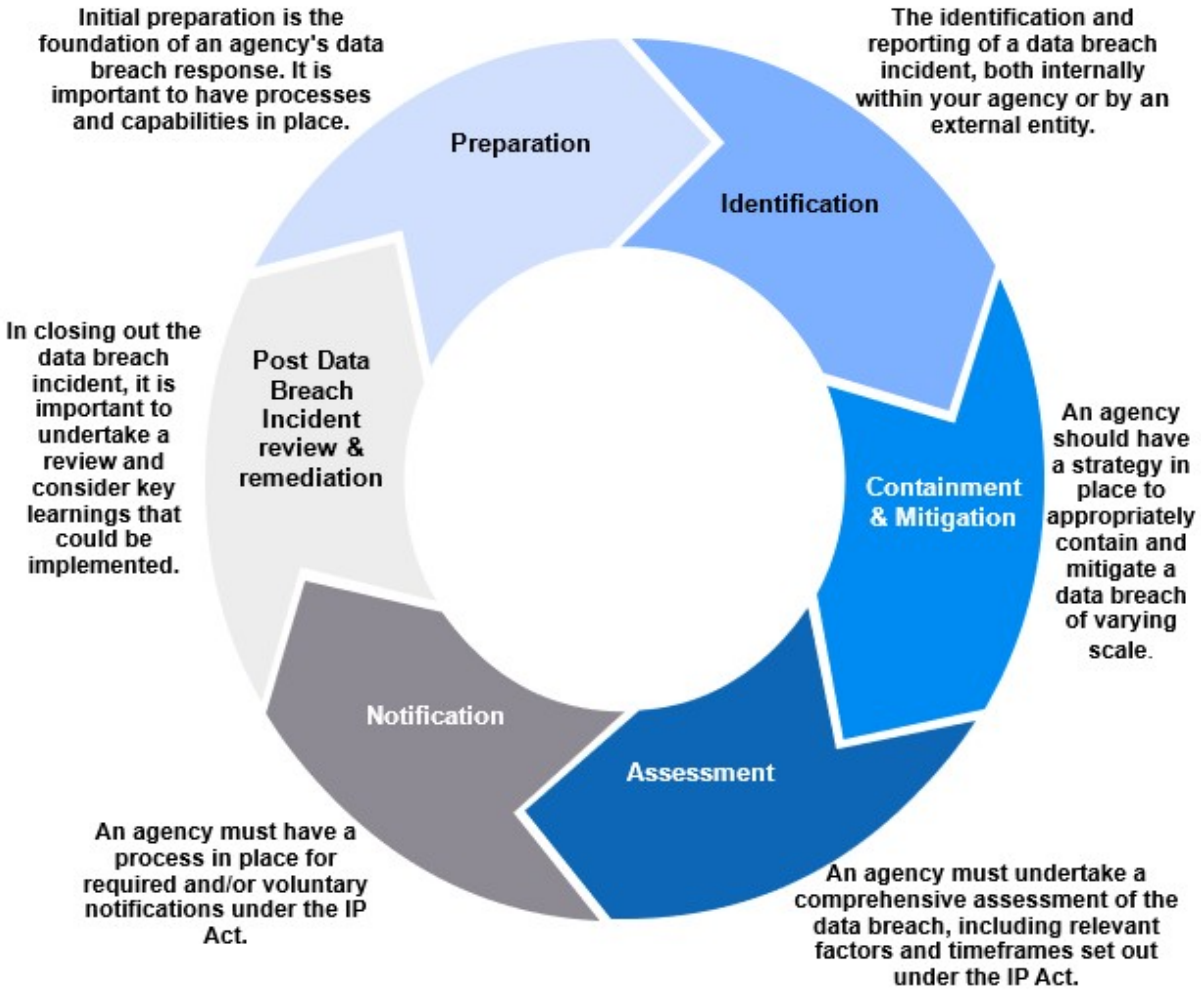
All Employees

All employees, contractors, volunteers and elected representatives must report suspected breaches immediately to the Governance Team.

- Must report suspected breaches immediately to the Governance Team.
- Participate in privacy induction and refresher training.
- Follow Council's privacy protocols and data handling procedures.
- Cooperate with containment and assessment efforts during breach investigations.
- Maintain vigilance in identifying and escalating potential data breaches.

Breach Response Stages

There are six (6) stages to a Data Breach Response.



- During Stage 1, Council undertakes an appropriate level of preparatory actions to ensure that data breaches can be appropriately addressed.
- Council will ensure that appropriate policies, procedures and systems are in place to identify data breaches and report them appropriately.
- Council will also identify internal officers and their roles and responsibilities in the case of a reported data breach.

- When a staff member becomes aware of a suspected or actual data breach, they must report it immediately to the Governance Team.
- Staff must report the breach in writing via email to governance@ccrc.qld.gov.au. All reports of a data breach must include the date, nature of the breach, affected data and any immediate actions taken.
- The Governance Team must assess the data breach in accordance with Council's risk management framework, identify the appropriate escalation, resourcing and communication to be adopted based on the risk level of the breach.

Risk Assessment Criteria
The following table outlines the risk levels and corresponding actions required:

Risk Level	Description	Action Required
Low	Minimal impact, no sensitive data	Monitor and document
Medium	Some personal data, limited exposure	Contain and notify internally
High	Sensitive data, likely harm	Notify affected individuals and OIC

Once the data breach has been identified, the Governance Team and Manager ICT will take steps to limit the breach, including disabling access, recovering records, and securing systems.

During Stage 4, the Governance Team will assess the breach to determine:

- The type and sensitivity of personal information involved.
- The cause and the extent of the breach.
- Whether serious harm is likely.
- Whether the breach meets the threshold for mandatory notification under IPOLA. (https://oic.advancedforms.squiz.cloud/form/mandatory-notification-data-breach-mndbscheme)

If the breach is deemed to be an 'eligible data breach', the following must occur:

- The Governance Team, following CEO approval, will notify affected individuals as soon as practicable.
  - Sample notification to affected individuals: "*We are writing to inform you of a recent data breach involving your personal information. The breach occurred on [date] and involved [brief description]. We have taken steps to contain the breach and are working to prevent recurrence. For support, contact [contact details].*"

- The Governance Team, with CEO approval, notify the Queensland Information Commissioner office.
    - Sample notification to the Commissioner: "*Winton Shire Council reports an eligible data breach under IPOLA. The breach occurred on [date], involved [data type], and affected [number] individuals. Containment and remediation actions have been initiated.*"
- The Governance Team will provide details of the data breach, the affected data and recommended actions to the CEO and Executive Leadership Team.
- The Governance Team will prepare a complaint response strategy for privacy complaints in preparation for privacy complaints that may arise.
-

Following a data breach incident, the CEO, Governance Team, Manager ICT and other appropriate employees will:

- Review the incident and the response effectiveness.
- Update procedures and systems to prevent recurrence. Considering the steps required to resolve the incident, the changes/controls that can/will prevent a breach occurring again.
- If necessary, review and update officers responsible for overseeing the review and remediation process.
- Review and update the process of managing the data breach, where required.
- Provide staff training if required.

CCRC data breach response process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. The initial response team consists of the Governance Team and the Manager ICT (or delegate).

There are four key steps to consider when responding to a breach or suspected breach.

- Step 1: Contain the breach
- Step 2: Assess the risks associated with the breach
- Step 3: Consider breach notification
- Step 4: Review the incident and take action to prevent future breaches

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. At all times, the response team should consider whether remedial action can be taken to reduce any potential harm to individuals.

The response team should refer to the checklist below and to the OIAC's Data Breach Preparation and Response, which provides further detail on each step.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

Following serious data breaches, the response team should conduct a post-breach review to assess the CCRC's response to the breach and the effectiveness of this plan and report the results of the review to the CRCC Executive Leadership Team. The post-breach review report should identify any weaknesses in this response plan and include recommendations for revisions or staff training as needed. As part of the review the response team should refer to the OAIC's Guide to Securing Personal Information.

The response team should also consider the following documents where applicable:

- CCRC Business Continuity Plan
- ICT Incident Response Plan
- CCRC Disaster Recovery plan

Third-Party Breach Handling

Contractors and service providers must report breaches to Council within 24 hours.
Contracts must include clauses requiring compliance with Council's data breach procedures

Testing this plan

Members of the response team should test this plan with a hypothetical data breach annually to ensure that it is effective. As with the post-breach review following an actual data breach, the response team must report to the OAIC Executive on the outcome of the test and make any recommendations for improving the plan.

Records management

In accordance with IPOLA and Council's record keeping policies, all data breaches and response actions will be documented through a Data Breach Register. The following fields should be included in the Data Breach Register:

- Date of breach
- Description
- Affected data
- Individuals impacted
- Actions taken
- Outcome
- Review date

Documents created by the response team, including post-breach and testing reviews, should be saved and registered in ECM.

Training and Awareness

All staff are to receive annual training on data breach identification, reporting and response procedures. Updates to legislation and acts will be provided to all staff where needed.

Reporting

Council's privacy management includes reporting to Executive Leadership Team meetings at least once each quarter and include a report of any privacy complaints against and internal data breaches.

A Register of Eligible Data Breaches will be maintained by Governance as required by the IPA.

Related forms, policies and procedures	Code of Conduct for Council Employees Councillor Code of Conduct Information Privacy and Confidentiality Policy CCRC Business Continuity Plan ICT Incident Response Plan CCRC Disaster Recovery plan
Relevant legislation	*Information Privacy Act 2009* *Information Privacy and Other Legislation Amendment Act 2023* *Human Rights Act 2019* *Privacy Act 1988 (Cth)* *Public Records Act 2023* *Right to Information Act 2009* *Qld government Information security policy (IS18:2018)*
Reference and resources	Office of Australian Information Commissioner Notifiable Data Breaches Scheme Queensland Government Chief Information Office

Policy Number	11049		
Approved by	Council Resolution LG0746	**Approval date**	23 July 2020
Approved by	Chief Executive Officer	**Approval date**	16 December 2022
Approved by	Manager Governance, Risk & Performance	**Approval date**	16 August 2023
Approved by	Chief Executive Officer	**Approval date**	19 February 2026
Review date	February 2026		