Banana Shire Council
Adopted: 11 June 2026

DATA BREACH RESPONSE PLAN

INTRODUCTION

Banana Shire Council (Council) has obligations under the *Information Privacy Act 2009* (IP Act) to protect personal information in its possession and control.

This Data Breach Response Plan (Response Plan) outlines the steps Council (Council) will follow in the event of a data breach involving personal information. This Response Plan aligns with the *Information Privacy Act 2009*, the *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA) and the *Queensland Privacy Principles* (QPPs).

PURPOSE AND SCOPE

The purpose of this plan is to set out the procedure to be followed by Council staff to ensure a timely, coordinated and compliant response to all data breaches, including mandatory notification where required.

This plan applies to all Council employees, contractors, volunteers and Councillors who handle personal information on behalf of Council.

Note: Where a data breach arises because of an information security incident (e.g. malware, ransomware) this plan must be read in conjunction with Council's Cyber Security Response Plan.

LEGISLATION

Crime and Corruption Act 2001
Information Privacy Act 2009
Information Privacy and Other Legislation Amendment Act 2023
Privacy Act 1988 (Cth)

RELATED DOCUMENTS
Queensland Privacy Principles

DEFINITIONS

Assessment	Evaluation of the data breach's cause, impact and notification requirements.
Containment	Actions taken to limit, isolate and prevent further unauthorised access, data loss or system compromise after a breach has been identified.
Data breach	Defined in the IP Act to mean the unauthorised access or disclosure of information held by an agency or the loss of

	personal or non-personal information held by an agency where unauthorised access or disclosure is likely to occur.
Eligible data breach	*Always* involves personal information and involves an actual or potential loss of unauthorised access to, or unauthorised disclosure of personal information, which is "likely to result in serious harm" to one person or more.
EMT	Executive Management Team
HR	Human Resources
LGMS	Local Government Mutual Services
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.
Notification	Informing affected individuals and authorities about a data breach.
Remediation	Actions taken to eliminate the root cause of the breach, correct vulnerabilities and restore systems and processes to a secure state after containment has been achieved.

ROLES AND RESPONSIBILITIES

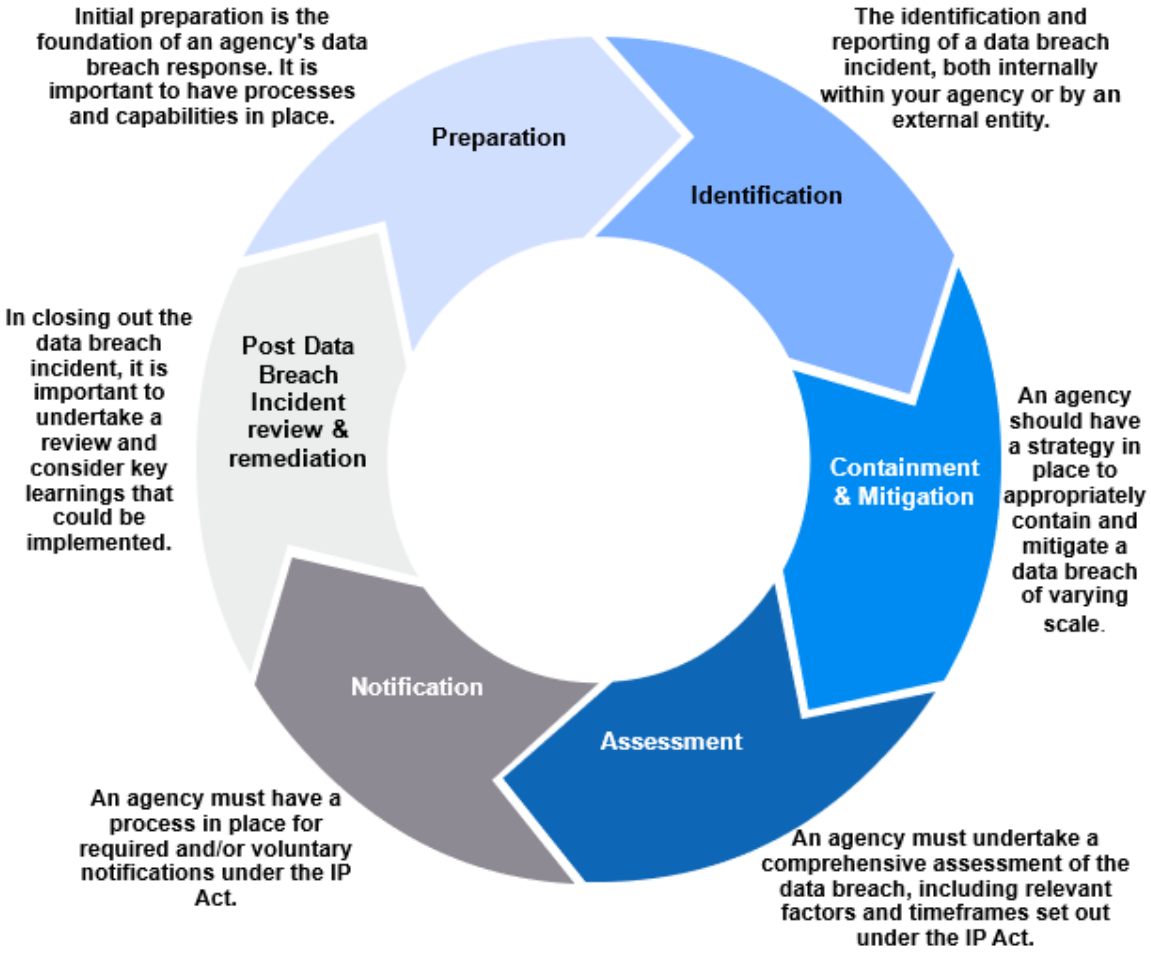
Chief Executive Officer (CEO)	• Provides strategic oversight of all breach responses. • Authorises post-incident reviews and remediation plans.
Governance Team	• Lead breach assessment and notification processes. • Coordinates internal reporting and documentation of breach incidents. • Liaises with the Office of the Information Commissioner (OIC) for mandatory notifications and compliance queries. • Maintains and updates the Data Breach Response Plan. • Oversees data breach and privacy training and awareness programs for staff. • Conducts post-breach reviews and ensures lessons learned are documented and actioned.
Information and Communication Technology (ICT) Team	The ICT team assists with technical containment, response and investigation of all breaches. • Identifies and contains technical aspects of the breach (e.g. 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 Staff	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 and data breach induction and refresher training. • Follow Council's privacy procedures and data handling procedures. • Cooperate with containment and assessment efforts during breach investigations. • Maintain vigilance in identifying and escalating potential data breaches.

RESPONDING TO A DATA BREACH

There are six stages to a Data Breach Response:

- **Stage 1** – Preparation
- **Stage 2** – Identification
- **Stage 3** – Containment & mitigation
- **Stage 4** – Assessment
- **Stage 5** – Notification
- **Stage 6** – Post-data breach incident review & remediation



Council may undertake some of these stages concurrently when responding to a data breach.

The scale and scope of the activities that Council may take will depend on the level of complexity, resources, expertise and experience in responding to data breaches.

Stage 1: Preparation

During Stage 1, Council will:

- Undertake an appropriate level of preparatory actions to ensure data breaches can be appropriately addressed.
- Ensure appropriate policies, procedures and systems are in place to identify data breaches and will report them appropriately.
- Ensure there is a broad awareness across Council of the policies, procedures and reporting obligations in place.
- Identify internal officers and their roles and responsibilities in the case of a reported data breach.

Stage 2: Identification

When an employee becomes aware of a real or a suspected data breach, they must report it immediately to the Governance team, their immediate Supervisor and Manager.

The breach must be reported in writing, via email to governance@banana.qld.gov.au. All reports must contain the following information:

- Date
- Nature of the breach
- Affected data
- Any immediate actions taken.

The Governance team must undertake a preliminary assessment of 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 and Notification Pathway
Low	Minimal impact, no personal or sensitive data released	Monitor and document
Medium	Some personal data, limited exposure, unlikely serious harm to an individual	Contain and document. Notify internally as required e.g. Governance/ITC/HR
High	Significant personal or sensitive data, likely serious harm to an individual	Assemble the Data Breach Response Team. Notify affected individuals and Office of the Information Commissioner

Stage 3: Containment and Mitigation

Depending on the nature of the data breach and where possible, the relevant staff member must take all reasonable steps to contain or prevent further damage from the breach.

Examples of containment include:

Unauthorised disclosure of personal information to a third party	• Recall emails sent to a wrong address, if possible; otherwise, ask the email recipient/s to delete the email from their Inbox and Recycle Bin/Trash and confirm when they have done so. • Arrange to collect any mail sent or delivered to an incorrect address. • Ask recipients not to use or disclose the information; consider whether to advise them about any applicable confidentiality obligations and the possible consequences of breaching those obligations.
Loss of device or physical files	• Recover the device or records (e.g. retrieve records left at a site).

	• Arrange to have the mobile device remotely disabled or wiped remotely. • Arrange a search of the site where the loss occurred (e.g. by contacting public transport, airline). • Notify the police, if appropriate.
Data breach involving electronic records on ICT system	• Isolate the causes of the breach in the relevant system, software or database. • Shut down the system that was breached and change computer access codes. • Reset log-in details and passwords for compromised devices, systems or databases. • Quarantine any compromised devices. • Instruct employees to immediately cease a particular practice.

If the recipient is subject to confidentiality obligations (e.g. a Council employee) and refuses to return documents or devices, or there are concerns that they might disseminate the information, consider whether it is appropriate to remind them of their confidentiality obligations.

Depending on the circumstances, consider whether to ask the third party to complete a statutory declaration attesting that they have returned, deleted or destroyed the information and any copies.

In response to a serious cyber security incident, it may be appropriate to engage an external cyber support service. Refer to the Cyber Security Response Plan for guidance.

Stage 4: Assessment

The Governance team will assess the data breach against the criteria prescribed under the IP Act to determine if the data breach is an Eligible Data Breach. If the data breach does involve personal information, the Governance team will gather information and determine the likelihood of serious harm, having regard to:

- The kind of personal information involved.
- The sensitivity of the information.
- If the information is protected by one or more security measures.
- The likelihood measures could be overcome.
- Person (or kinds), of have obtained, or who could obtain, the personal information.
- The nature of the harm like to result from the date breach.
- Depending on the circumstances, any other relevant matter, like how long information was exposed, circumstances of affected individual, how it occurred, combinations of personal information and actions taken by Council to reduce the risk of harm.

The Office of the Information Commissioner's MNDB assessment tool can be used to determine whether a data breach is an eligible data breach under the IP Act.

Stage 5: Notification

If the data breach is determined to be an eligible data breach, the following notifications will occur:

Officer/Team	Action	Approving officer	Notification type
Governance Team	Notify affected individuals.	Manager Governance	External
ICT Team (Cyber Incident)	Notify affected individuals.	Manager Information and Communication Technology	External
Manager Governance	Notify the office of the Queensland Information Commissioner.	CEO	External
Governance Team / ICT Team (Cyber Incident)	Liaise with Media team to prepare communication strategy for external communications.	CEO	External
Governance Team	Consider other notifications obligations e.g. corrupt conduct under the *Crime and Corruption Act 2001*, Tax file numbers under the *Privacy Act 1988*, Queensland Police Service if criminal conduct.	CEO	External
Insurance and Risk Team	Notify Council's insurance provider (LGMS) if the data breach incident is likely to expose Council to damages claims.	Manager Governance	External
Governance Team	Prepare report to CEO and EMT covering details of the data breach, affected data and recommended actions.	Manager Governance	Internal
ICT Team (Cyber incident)	Prepare report to CEO and EMT covering details of the data breach, affected data and recommended actions.	Manager Information and Communication Technology	Internal
Governance Team	Prepare complaint response strategy for any privacy complaints that may arise.	Manage Governance	Internal

Stage 6: Post-incident review

Following the data breach, the CEO, Governance team, ICT team, and other relevant employees will:

- Review the incident and the response plan effectiveness.
- Update procedures and systems to prevent recurrence. Consider the steps to resolve the incident, the changes/controls that can/will prevent a breach occurring again.
- If necessary, review and update officers responsible for the review and remediation process.
- Consider potential legal issues, including liability, compensation, insurance and other legal and regulatory issues, such as human rights that should be considered in the review and remediation process.
- Provide staff training, if required.

THIRD-PARTY BREACH HANDLING

Contractors and service providers must report breaches to Council within 24 hours of becoming aware of a data breach. Council's contracts include clauses requiring service providers to comply with the IP Act.

ESCALATION PATHWAYS

Breaches assessed as high risk must be escalated to the CEO within 24 hours. The Governance team will coordinate all communication and responses.

RECORDKEEPING

Council will maintain all records in accordance with Council's Records Management Policy and Procedures. Council will maintain a Data Breach Register that will include:

- Data breach identifier.
- Description of data breach.
- Date statement provided to OIC.
- Date further information requested from OIC.
- Notification to individuals.
- Application of any exemptions.
- Description of steps taken to contain and mitigate harm.
- Description of preventative actions taken.

TRAINING AND AWARENESS

All staff will receive general awareness training on data breach identification, reporting and response procedures. Training and awareness will be provided by way of internal emails, staff newsletters and in-person where required.

REVIEW AND AUDIT

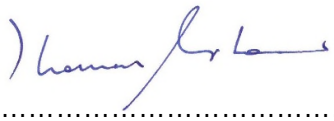
This plan will be reviewed every two years, or earlier if required by legislative changes or internal reviews.

This Council Plan acknowledges the importance of fundamental human rights.

Council is committed to recognising and protecting these rights when creating policies and procedures that shape the frameworks, standards, behaviours, and actions of the Banana Shire Council.

An assessment of this Plan determined that it does not limit or affect any human rights under the *Human Rights Act 2019*.

CERTIFICATION



…….
CHIEF EXECUTIVE OFFICER
BANANA SHIRE COUNCIL

17 June 2026
…….
DATE

ATTACHMENT 1 - GLOSSARY OF COMMONLY USED TERMS

Eligible data breaches can have a number of different causes, e.g. human error, malicious actions, or system faults, which different agencies may describe in different ways.

The glossary in the below table, will assist Council to accurately and consistently:

- categorise the causes of data breaches
- accurately identify and describe data breach causes; and
- contain and mitigate potential harm.

Common Human Error Causes	Definitions
Human Error	**An unintended action by an individual directly resulting in a data breach.**
Failure to use Blind Carbon Copy (BCC) when sending email	Sending an email to a group of people and placing all recipient emails addresses in the 'To' field, thereby disclosing all recipient email addresses to all recipients
Failure to redact personal information	Failure to de-identify and/or delete personal information from a document record before it is disclosed
Incorrect personal information attached to a file	Personal information is attached to a client file which is then subsequently accessed or disclosed
Insecure disposal	Disposing of personal information documents in a manner that results in unauthorised loss or disclosure. For example, placing documents in a public bin to dispose of customer records instead of the secure disposal bin
Loss of paperwork or data storage device	The physical loss of personal information. This may be where an employee accidently leaves a client folder on a train or leaves a work laptop in a taxi
Personal information sent to the wrong recipient	Personal information sent to the wrong recipient via email, fax, post, courier service or other electronic method
Unauthorised access	Where personal information is accessed without authority or a purpose that is not directly related to the persons duties or work functions
Unauthorised verbal disclosure	Verbally sharing personal information without authorisation. This may include sharing or openly discussing sensitive medical information in a hospital waiting room
Unauthorised disclosure by unintended release or publication	Unauthorised disclosure of personal information in writing, sending a letter to the wrong address, but with the correct name or publishing information online
Common Malicious or Criminal attacks	**Definitions**
Malicious or Criminal attacks	**A malicious or criminal attack, deliberately crafted to exploit known vulnerabilities for financial or other gain**
Theft of paperwork or data storage device	Theft of a physical device or paperwork containing personal information
Social engineering/impersonation	Directed attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices to gain access to systems, networks or physical locations
Rogue employee/insider threat	Intentional attack by an employee or insider (e.g. contractor) conducting activities that are not in the interest of the employer or other entity
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices
Malware	Short for 'malicious software'. Software used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malware include trojans, viruses and worms
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment

Phishing (compromised credentials)	Untargeted, mass messages sent to many people asking for information, encouraging them to open a malicious attachment, or visit a fake website that will ask the user to provide information or download malicious content
Brute force attack	A typically unsophisticated and exhaustive process to determine a cryptographic key or password that proceeds by systematically trying all alternatives until it discovers the correct one
Compromised or stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown
Hacking	Unauthorised access to a system or network (other than by way of phishing, brute-force attack, or malware), often to exploit a system's data or manipulate its normal behaviour
Business email compromise	A form of cybercrime that uses email fraud to attack an organisation to achieve a specific outcome that negatively impacts the target organisation
Common System Fault Causes	**Definitions**
System Fault	**A business or technology process error not caused by direct human error**
Mail merge failure	A system failure which results in personal information being misdirected to the incorrect individual
Unintended release or publication	A system failure which results in the release or publication of personal information