ORDINARY MEETING 27 MAY 2026	5.3

ADOPTION OF INFORMATION PRIVACY, RIGHT TO INFORMATION AND DATA BREACH GENERAL POLICIES

POP | 65/4/1-07 | #7874203

RECOMMENDATION:

That Council adopts the Information Privacy General Policy, Right to Information General Policy and Data Breach General Policy.

INTERESTED PARTIES:

Not applicable

EXECUTIVE SUMMARY:

The *Information Privacy and Other Legislation Amendment Act 2023* introduced significant reforms to Queensland's privacy and information management framework. Most amendments commenced on 1 July 2025, with remaining obligations for local government, including Mandatory Data Breach Notification, commencing on 1 July 2026.

To support Council's compliance with these legislative changes, three new policies have been developed:

- Information Privacy General Policy
- Right to Information General Policy
- Data Breach General Policy

These policies establish a robust governance framework for how Council manages personal information, responds to access applications, and identifies and manages data breaches. Endorsement of these policies will ensure Council meets its statutory obligations under the *Information Privacy Act 2009* and *Right to Information Act 2009*, while strengthening transparency, accountability and public trust.

BACKGROUND:

The *Information Privacy Act 2009* regulates how Queensland public sector agencies, including local governments, collect, store, use and disclose personal information. The *Information Privacy and Other Legislation Amendment Act 2023* introduced key reforms to modernise this framework. A significant change is the replacement of the previous Information Privacy Principles (IPPs) with a single set of Queensland Privacy Principles (QPPs). These principles align more closely with contemporary privacy expectations and national standards.

In addition, the reforms introduce a Mandatory Data Breach Notification scheme, requiring public sector agencies to assess and notify affected individuals and the Office of the Information Commissioner where an eligible data breach occurs. This requirement will apply to local governments from 1 July 2026.

These changes require Council to update and formally adopt policies to ensure compliance with both existing and emerging legislative obligations.

COMMENTS:

The proposed policies collectively establish a clear and consistent framework for the management of personal information and access to information across Council.

Information Privacy General Policy
This policy outlines how Council manages personal information in accordance with the *Information Privacy Act 2009* and the Queensland Privacy Principles. It applies to Councillors, employees and contracted service providers. The policy addresses the full information lifecycle, including collection, use, disclosure, storage and security of personal information.

Right to Information General Policy
This policy supports Council's commitment to transparency and open government by outlining how the community can access information held by Council. It reinforces the principles of proactive disclosure and sets out Council's approach to formal applications under the *Right to Information Act 2009* and the *Information Privacy Act 2009*.

Data Breach General Policy
This policy establishes a structured approach to identifying, assessing and responding to data breaches. It sets out roles and responsibilities, reporting requirements, and escalation processes, and prepares Council for the commencement of Mandatory Data Breach Notification obligations from 1 July 2026.

Together, these policies strengthen Council's information governance framework and provide clear guidance to staff on their obligations when handling personal information.

OPTIONS:

Option 1: (Recommended)

That Council adopts the Information Privacy General Policy, Right to Information General Policy and Data Breach General Policy.

Option 2:

That Council does not adopt the proposed Information Privacy General Policy, Right to Information General Policy and Data Breach General Policy. This would impact Council meeting its legislative obligations.

CONSIDERATIONS:

Risk Management:

The adoption of these policies forms a key component of Council's risk management framework by strengthening controls around the collection, use, disclosure and protection of personal information. The policies support compliance with legislative obligations under the *Information Privacy Act 2009* and prepare Council for forthcoming Mandatory Data Breach Notification requirements.

Effective implementation, supported by staff training, clear procedures and ongoing monitoring, will reduce the likelihood and impact of privacy breaches, improve consistency in decision making, and enhance Council's ability to respond to incidents in a timely and transparent manner.

Corporate and Operational Plans:

The adoption of these policies aligns with Council's strategic objectives outlined in the Corporate Plan 2025–2030 by supporting effective community outcomes through strong governance and informed decision making. This contributes to Focus Area 5: Focused Council, which prioritises collaborative, transparent and accountable decision making, as well as the implementation and continuous improvement of a contemporary governance framework.

Statutory:

The proposed policies ensure continued compliance with all relevant legislative frameworks.

CONSULTATION:

Consultation was undertaken with key internal stakeholders during the development of these policies. The policies were also workshopped with Councillors.

ATTACHMENTS:

Attachment 1: Information Privacy General Policy #7828453
Attachment 2: Right to Information General Policy #7828083
Attachment 3: Data Breach General Policy #7828094

Mandy Wise
Executive Manager Organisational Performance

Holly Mc Bride
Director People and Organisational Performance

CAIRNS REGIONAL COUNCIL

General Policy

INFORMATION PRIVACY

Intent The intent of this policy is to set out how Cairns Regional Council (Council) will manage and protect the personal information of individuals in accordance with the *Information Privacy Act 2009* and the Queensland Privacy Principles (QPPs).

Scope Applies to all Councillors, employees, contractors and volunteers of Council, and to all personal information collected, created, stored, used or disclosed by Council in performing its functions. This includes information held in Council systems, technologies and public records, whether managed by Council, its employees or contracted third parties.

DEFINITIONS

Term	Definition
Access	Providing an individual with personal information that is held by Council. Access may include allowing that individual to inspect (view) personal information or to obtain a copy of the personal information.
Anonymity / Pseudonymity	Options for individuals to interact with Council without revealing their identity, where lawful and practicable.
Authorised Officer	A Council employee or contractor who has been given authority to collect, use, access, or disclose personal information as part of their official duties.
Collection	The act of obtaining personal information for Council's functions, whether directly from the individual or via a third party.
Confidential Information	Information obtained or generated through Council activities that is not publicly available and has restrictions on access or disclosure under law, contract or Council policy.
Consent	A voluntary agreement (express or implied) to some act or practice which impacts an individual's personal information. An individual must be adequately informed before giving consent and must have the capacity to understand and communicate their consent.
Contracted Service Provider	An external provider contracted to deliver services for Council who may collect, store, use or disclose personal information on Council's behalf.
Councillors	All elected representatives who holds (current) office with council, including the mayor.
Data Breach	Any unauthorised access to, disclosure of, or loss of personal information that could cause harm to an individual.
De-identify	To remove or modify personal information so that no individual can reasonably be identified.
Disclosure	Making personal information available to someone outside Council, whether intentionally or unintentionally, including to another agency, entity or individual.
Information Privacy Act 2009 (IP Act)	Queensland legislation that regulates how Queensland public sector agencies manage personal information.

Term	Definition
Law Enforcement Activity	Activities carried out by law enforcement agencies that require the use or disclosure of personal information under QPP 6.
Mandatory Notification of Data Breaches (MNDB) Scheme	A statutory scheme commencing 1 July 2026 that requires local governments to notify affected individuals and the Office of the Information Commissioner of eligible data breaches involving personal information.
Personal Information	Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identifiable individual or an individual who is reasonably identifiable (as defined in the IP Act).
Primary Purpose	The purpose for which personal information was originally collected.
Public Record	Information created, received or kept by Council in the course of its operations that provides evidence of decisions or activities, as defined under the Public Records Act 2023.
Queensland Privacy Principles (QPPs)	The principles set out in the IP Act that govern how Council must collect, store, use, disclose and manage personal information.
Right to Information Act 2009 (RTI Act)	The Act that provides individuals the right to access and amend documents held by Council, unless exempt or contrary to the public interest.
Secondary Purpose	A purpose other than the primary purpose, permitted only where allowed under the IP Act.
Sensitive Information	A subset of personal information that includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation, or criminal record (as recognised in the IP Act).
Unsolicited Personal Information	Personal information received by Council that was not requested or intentionally collected.
Use	Handling personal information within Council, including internal analysis, referencing, reporting, or decision-making.

PROVISIONS

Principles

Council recognises privacy as a fundamental human right and is committed to protecting personal information in accordance with the *Information Privacy Act 2009* (IP Act) and the Queensland Privacy Principles (QPPs).

The QPPs set out how Queensland public sector agencies, including local governments, must collect, store, use and disclose personal information under the IP Act. They require Council to collect only what is necessary, to inform individuals about why their information is being collected, to ensure information is accurate and secure, and to use or disclose it only for authorised purposes. The QPPs also give individuals rights to access and amend their personal information and require Council to manage personal information transparently and responsibly.

The QPPs are based on the 13 Australian Privacy Principles (APPs) but not all APPs were implemented into the IP Act. The following QPPs are not used under the IP Act:

- QPP 7 – Direct Marketing
- QPP 8 – Cross-border disclosure of personal information, noting that similar requirements to APP 8 are contained in section 33 of the IP Act.
- QPP 9 – Adoption, use or disclosure of government related identifiers.

Open and Transparent Management of Personal Information (QPP 1)
Council manages personal information in an open and transparent way and uses it only for the purpose of conducting Council business. Council will ensure compliance with the QPPs by developing, maintaining and implementing processes that assist individuals to make enquiries or complaints about Council's compliance with the IP Act. This Privacy Policy will be available at Council's Customer Service Centre and on Council's website.

Anonymity and Pseudonymity (QPP 2)
Where possible, individuals have the option of not identifying themselves or of using a pseudonym when dealing with Council. Circumstances where anonymity is not available include:

- where Council is required or authorised by an Australian law, or a court or tribunal order, to deal only with identified individuals; or
- where it is impracticable for Council to respond to or action the matter without identifying the individual.

In some cases, Council may not be able to progress a request, complete an investigation or provide a response unless the individual's identity is known.

Collection of Solicited Personal Information (QPP 3)
Council only collects personal information where it is necessary for a lawful Council function or activity. Personal information is collected lawfully and fairly, and only where the collection is reasonably necessary for Council to deliver services, carry out regulatory responsibilities or perform other statutory functions.

Council may also collect sensitive information and will generally only collect sensitive information directly from the subject individual or with their consent, or otherwise consistent with Council's obligations under the IP Act.

Dealing with Unsolicited Personal Information (QPP 4)
Where Council receives personal information that it did not solicit, Council will consider whether the information could have been collected under QPP 3. If Council determines it could not have collected the information, and subject to the *Public Records Act 2023*, Council will, where lawful and reasonable, destroy or de-identify the information in accordance with the QPPs and authorised retention and disposal schedules.

Notification of the Collection of Personal Information (QPP 5)
Council will not collect personal information about an individual unless:

- Consent is provided by the individual; or
- It is required by Council to fulfil its responsibilities, or to provide services and facilities to individuals or collection is required by law; or
- Collection is necessary to prevent or lessen a serious threat to life, health, safety or welfare of an individual or to public health, safety or welfare.

Council also informs individuals about this Privacy Policy and how they can access it.

Use or Disclosure of Personal Information (QPP 6)
Council may use or disclose personal information for a purpose other than the original purpose of collection only where permitted under the IP Act. This includes circumstances where:

- the individual has provided consent
- Council is authorised or required under an Australian law to use or disclose the information
- the secondary use or disclosure is reasonably expected and related to the primary purpose (or, in the case of sensitive information, directly related)
- the information is reasonably necessary for one or more law enforcement activities.

Council may also use or disclose personal information for approved research or statistical purposes where:

- the use or disclosure is in the public interest
- the information will not be published in a way that identifies individuals
- it is not practicable to obtain consent
- Council is satisfied the receiving entity will not further disclose the information.

Where Council uses or discloses personal information for law enforcement activities, Council will make a written note of the use or disclosure. This may include disclosure to a court or tribunal.

Quality of Personal Information (QPP 10)
Council takes all reasonable steps to ensure personal information it uses or discloses is accurate, complete and up to date, having regard to the purpose of its use.

Security of Personal Information (QPP 11)
Council takes reasonable steps to protect personal information from misuse, loss, unauthorised access, unauthorised use, modification or disclosure. Access to Council systems is restricted to authorised staff using secure authentication methods. Council will destroy or de-identify personal information when:

- it is no longer required for the purposes permitted under the QPPs
- the information is not contained in a public record
- Council is not required to retain it under an Australian law or court order.

Access to and Correction of Personal Information (QPP 12 and 13)
Individuals may apply to access their personal information under the *Right to Information Act 2009* (RTI Act). Council will provide access unless required or authorised to refuse access under the RTI Act or another law. Individuals may request amendment of their personal information if it is inaccurate, incomplete, out of date, irrelevant or misleading.

If Council refuses to amend the information and the individual asks Council to associate a statement with the information, Council will take reasonable steps to ensure the statement is apparent to users of the information.

Privacy Complaints
An individual may make a privacy complaint if they believe Council has not handled personal information in accordance with the IP Act. A privacy complaint on behalf of another individual can be made only if authorised by that individual. A privacy complaint in relation to a minor/child may be made by a parent or guardian.

Privacy complaints must be lodged with Council in the first instance, and Council has 45 business days to respond. Council may request an extension of this timeframe where appropriate. If a complainant is dissatisfied with Council's handling of the complaint, or if Council does not respond within the required timeframe, the complainant may refer the matter to the Office of the Information Commissioner.

Data Breach
Council recognises the significant responsibility that comes with handling personal information and is committed to protecting it at all times. To support strong information governance practices and to meet our obligations under the IP Act and the Mandatory Notification of Data Breach (MNDB) scheme, Council has established a Data Breach Policy which outlines how Council prepares for, identifies, assesses, contains, notifies, and reviews data breaches involving information in our possession or control.

Human Rights
When collecting, storing, using or disclosing personal information, Council must consider any potential impacts on the human rights of individuals, including the right to privacy and reputation. Decisions involving personal information must be justifiable, proportionate and consistent with the *Human Rights Act 2019* (Qld). Any limitation on human rights must be reasonable and demonstrably justified

Related Documents

Right to Information General Policy
Information Privacy General Policy
Data Breach General Policy
Code of Conduct for Councillors
Code of Conduct (Employees)

◆◆◆◆◆◆

This policy is to remain in force until otherwise determined by Council.

Director responsible for Review: **Director People and Organisational Performance**

ORIGINALLY ADOPTED: {Enter Date}
CURRENT ADOPTION: {Enter Date}
DUE FOR REVISION: {Enter Date}
REVOKED/SUPERSEDED: {Enter Date}

.....
Ken Gouldthorp
CHIEF EXECUTIVE OFFICER

CAIRNS REGIONAL COUNCIL

General Policy

RIGHT TO INFORMATION

Intent To support the community's right to access information held by Cairns Regional Council (Council) in accordance with the *Right to Information Act 2009* and the *Information Privacy Act 2009*. This policy ensures that access to information is facilitated in a timely, fair and responsible manner, while maintaining appropriate protections for confidential and personal information as required under legislation.

Scope Applies to Councillors and Council staff and contracted service providers handling Council information under service arrangements. For the purpose of this policy, Council staff includes employees, contractors, consultants, volunteers and any other individuals engaged to perform work on behalf of Council. It covers all Council information and "documents of an agency", regardless of format, location or storage medium.

DEFINITIONS

Term	Definition
Agency	Cairns Regional Council
Councillors	All elected representatives who hold (current) office with council, including the mayor.
Disclosure Log	A disclosure log is a part of an agency's website that publishes documents, or information about how to obtain them, after they have been released under a Right to Information (RTI) application. Its purpose is to improve public access to information and reduce duplicate applications. [oic.qld.gov.au]
Document of an Agency	A document in the possession or under the control of an agency, or the agency concerned, whether created or received in the agency, and includes— (a) a document to which the agency is entitled to access; and (b) a document in the possession or under the control of an officer of the agency in the officer's official capacity.
Processing charge	in relation to an application for access to a document, means the charge prescribed under a regulation for searching for or retrieving the document, or making, or doing things related to making, a decision on the application.
Relevant Third Parties	A third party is any government, agency or person whose information is contained in a document and who may reasonably be expected to be concerned about its release.

PROVISIONS

These provisions are to be read in accordance with the *Right to Information Act 2009* (RTI Act) and the *Information Privacy Act 2009* (IP Act). These Acts establish the community's right to obtain information held by Council while ensuring personal information and other confidential material is appropriately protected.

Principles

Council is committed to supporting community access to information, maximising the amount of corporate information that is publicly available, and fostering a culture of openness and transparency. Council will apply the pro-disclosure principle, releasing information administratively where appropriate and using formal RTI processes as a last resort. Privacy will be protected through compliance with the Queensland Privacy Principles (QPPs) and sound records governance.

The RTI Act establishes a public right of access to documents in Council's possession or under Council's control. In establishing this right of access, the RTI Act sets out specific processes that must be followed in seeking access to Council documents as well as the grounds of exemption which can apply to prevent the disclosure of certain Council information and documents.

Responsibilities

Role	Responsibilities
Chief Executive Officer	• The Principal Officer under the RTI Act. • Delegates RTI decision making authority to the Right to Information Officer.
Right to Information Officer	• Is the decision maker for RTI access applications. • Receives, assesses and processes RTI applications, including determining scope, ensuring compliance, coordinating searches and making (or preparing) decisions on access. • Advises the public on how to access information, including whether it is available administratively, through the publication scheme or via a formal RTI application. • Manages proactive disclosure obligations, such as maintaining the publication scheme and disclosure log, and ensuring released information is published appropriately. • Liaises with Office of the Information Commissioner (OIC)
Team Leader Information Governance	• Oversees RTI and privacy programs, publication scheme and disclosure log. • Undertakes internal reviews of RTI decisions. • Approves procedures, templates and staff training.
Councillors and Council Staff	• Comply with RTI Act, IP Act and QPPs to ensure Council meets its legislative obligations. • Comply with all RTI and IP requirements, including correct handling, storage and disclosure of information, and contributing to lawful, timely processing of RTI requests.

Role	Responsibilities
	• Create and maintain accurate records to enable effective searches and ensure complete, reliable information is available for RTI decision-making and public access. • Support openness and transparency by ensuring information is managed and disclosed in line with the RTI Act's pro-disclosure principles, while protecting confidential or exempt information where required.
Contractors and contracted service providers handling Council information under service arrangements.	• Comply with IP Act and QPPs. • Protect Council information and support secure information handling.

Publication scheme

Council will publish and maintain a publication scheme on its website. The scheme will describe Council's functions, the information it holds and releases, how the public can access it, and any applicable fees.

Disclosure Log

A disclosure log is a public record that shows what information Council has released under the RTI Act. Council will publish on its disclosure log documents released to applicants under RTI, after the applicant has accessed them or after the access period lapses, except where publication is not permitted or appropriate. Council will remove any information that is unlawful to publish, defamatory, an unreasonable invasion of privacy, confidential or commercially sensitive. Council will never publish an applicant's personal information.

Administrative Access

Administrative access applications are ad hoc requests for a Council document or part of a document. The administrative release of information is to be in accordance with open and transparent governance and can reduce the need for a formal RTI access application. An administrative access request must be referred to the Right to Information Officer for consideration. The Right to Information Officer will assess the request to determine whether information can be released informally in line with the RTI Act's pro-disclosure principles and relevant legislative requirements.

RIGHT TO INFORMATION PROCESS

Making an Application

Applications are to be made in writing and must contain sufficient information to identify the documents that the applicant is seeking access to. When an applicant makes an access application that is not valid, the Council must make reasonable efforts to contact the application to provide the applicant with a reasonable opportunity to make the application a valid application. Once the application becomes a valid application, the statutory processing period commences.

Timeframes and Processing Charges

Council will process applications within the statutory processing period, issue charge estimate notices where relevant and explain any extensions. The RTI Act provides Council with a 25 business day processing period from Council's receipt of a valid application to provide a written decision. Day one of the processing period starts on the next business day after the application is deemed valid. Decision notices will set out findings, reasons and review rights.

Searching for Documents

The RTI decision maker must make and document reasonable searches across all business systems, network drives, devices, email and off-site storage. Council will keep written search records to support decisions and any reviews.

Third-Party Consultation

Where disclosure may reasonably be expected to affect the interests of relevant third parties, Council will consult and consider their views before making a decision regarding access.

Grounds for Refusal or Redaction

Council may refuse access if information is exempt or contrary to the public interest, or if processing would unreasonably divert resources, consistent with the RTI Act. Where practicable, Council will provide redacted copies that remove exempt information.

Providing Access

Access will be provided in the form requested where reasonable and lawful, including via secure download links that remain available for at least the statutory access period.

Review Rights

Applicants will be advised of their internal review and external review rights through the Office of the Information Commissioner (OIC). It is not necessary to have an internal review before applying for an external review.

RELATED DOCUMENTS

Information Privacy General Policy

◆◆◆◆◆◆

This policy is to remain in force until otherwise determined by Council.

Director responsible for Review: **Director People and Organisational Performance**

ORIGINALLY ADOPTED: {Enter Date}
CURRENT ADOPTION: {Enter Date}
DUE FOR REVISION: {Enter Date}
REVOKED/SUPERSEDED: {Enter Date}

.....
Ken Gouldthorp
CHIEF EXECUTIVE OFFICER

CAIRNS REGIONAL COUNCIL

General Policy

DATA BREACH

Intent Cairns Regional Council (Council) recognises the significant responsibility that comes with handling personal information and is committed to protecting it at all times. To support strong information governance practices and to meet Council's obligations under the *Information Privacy Act 2009* and the Mandatory Notification of Data Breach (MNDB) scheme, Council has established a Data Breach Policy. This policy outlines how Council prepares for, identifies, assesses, contains, notifies, and reviews data breaches involving information in Council's possession or control.

Scope Applies to Councillors, Council employees, volunteers, and contractors and contracted service providers handling Council information under service arrangements.

DEFINITIONS

Term	Meaning
Affected individual	An "affected individual" under section 47(1)(ii) of the IP Act is an individual to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach.
Councillors	All elected representatives who hold (current) office with council, including the mayor.
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 Response Plan	A more detailed procedural document complementing the Data Breach Policy, which could be an internal document detailing Council's more specific processes in managing and responding to a data breach.
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 Council, 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 Council 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.
Information Commissioner	The Queensland Information Commissioner. The Office of the Information Commissioner is Queensland's independent body that oversees the administration of right to information and information privacy laws, ensuring

Term	Meaning
	agencies comply with their obligations and protecting the personal information of the community.
IP Act	The *Information Privacy Act 2009* (Qld).
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: (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.

PROVISIONS

Principles

Council is committed to protecting personal information and ensuring strong data governance. This policy aims to safeguard the privacy of individuals, protect Council information and minimise harm resulting from data breaches. Effective breach management helps reduce impacts on affected individuals and organisations, while also enabling Council to learn from incidents and strengthen its data protection measures.

Data Breach

A 'data breach' for the purpose of this policy means either of the following in relation to personal information held by Council:

- unauthorised access to, or unauthorised disclosure of, the information.
- the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

A data breach may occur through malicious or criminal activity, system faults, or human error, and can involve unauthorised access, unauthorised disclosure, or the loss of information where unauthorised access or disclosure is likely to occur.

<u>Malicious or criminal attack:</u>

- Cyber incidents such as ransomware, malware, hacking, phishing or credential-harvesting attempts that result in unauthorised access to, leakage of or theft of personal information.
- Social engineering or impersonation that tricks staff into inappropriately providing personal information to unauthorised individuals.
- Insider threats, where an employee or contractor intentionally abuses valid system access to view, use or disclose personal information beyond their delegated role or permissions.
- Theft or loss of physical assets containing personal information, such as laptops, mobile phones, USB drives, paper files or removable media.

System fault:

- System failures or configuration issues can inadvertently expose personal information.
- Software bugs or configuration errors that allow unintended system access without authentication or automatically generate correspondence containing the wrong personal information.
- Incorrect publication of information, such as a database, internal portal or document accidentally being made publicly accessible online.
- Automated notices (e.g., infringement notices, development application updates) being sent to incorrect recipients due to a system error.

Human error:

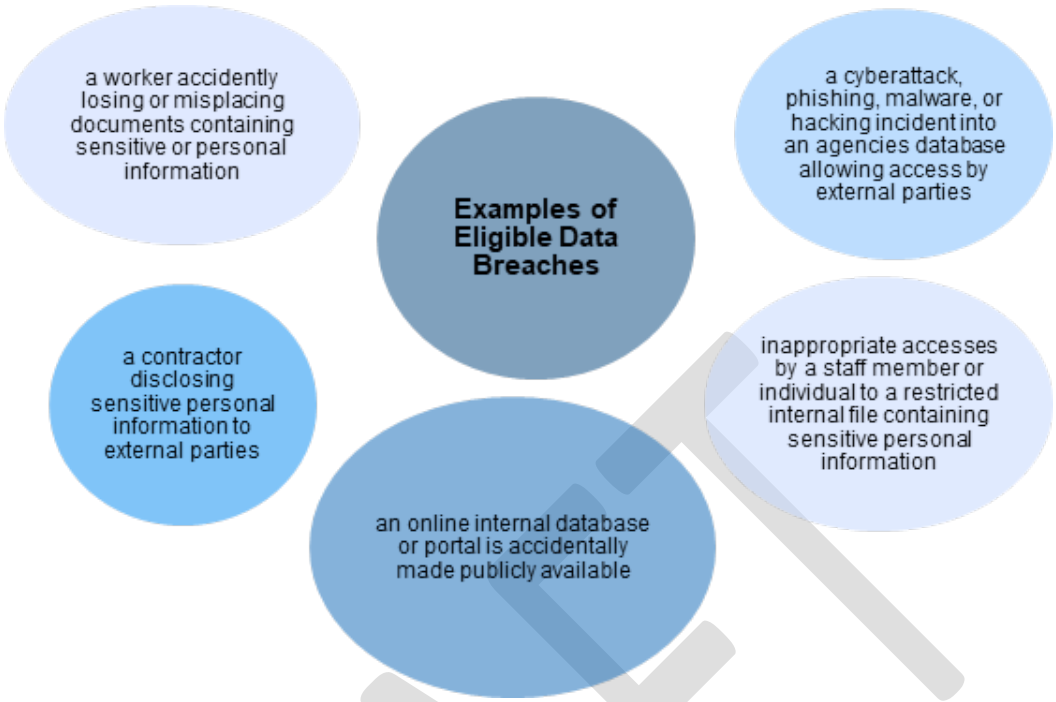
- Emailing or mailing information to the wrong recipient, including where attachments contain personal information not intended to be shared.
- Incorrect access permissions, where an employee or contractor is unintentionally granted access to systems or folders containing personal or sensitive information.
- Poor password or security practices, including sharing login credentials, not securing files, or failing to review or remove access when roles change.
- Accidentally losing or misplacing documents containing personal information, such as development application paperwork or complaint files.

Eligible Data Breach

A data breach becomes an Eligible Data Breach when it involves personal information likely to result in serious harm, such as financial, psychological or reputational harm. This includes situations where there has been actual unauthorised access or disclosure, as well as cases where information is lost and it is reasonably likely that such access or disclosure will occur.

In the event of a data breach Council is required to comprehensively assess the risks associated with the breach. As the *Information Privacy Act 2009* (IP Act) imposes specific obligations for an Eligible Data Breach, a Data Breach Policy needs to detail Council's assessment process for any data breach but also the process for specifically determining whether the data breach is an Eligible Data Breach for the purposes of the IP Act and the Mandatory Notification of Data Breach (MNDB) scheme.

Examples of Eligible Data Breaches. *Source: Office of the Information Commissioner*.



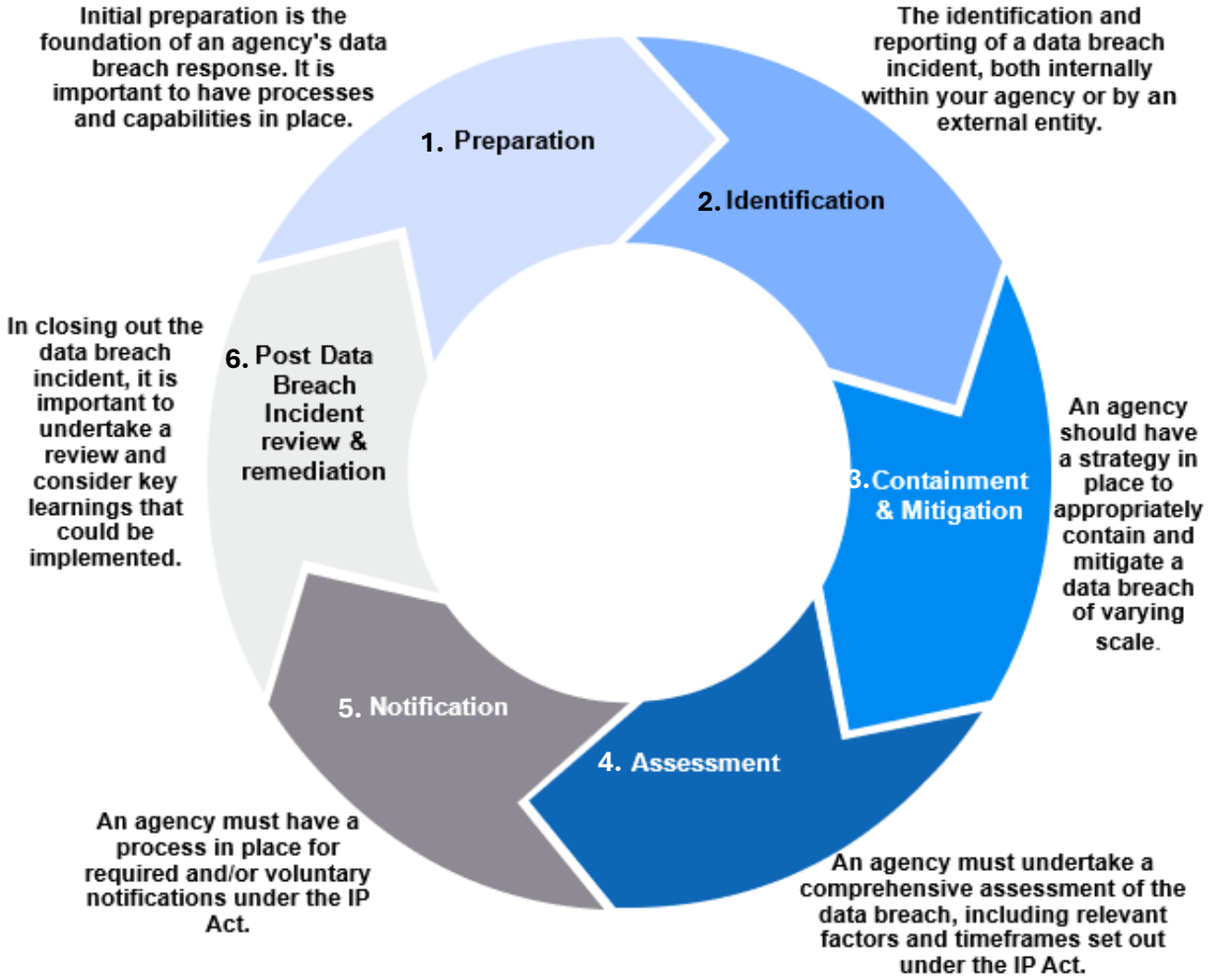
Data Breach Readiness, Response and Reporting

Council recognises that every data breach requires careful assessment and a response that fits the specific circumstances. Readiness involves maintaining up-to-date policies, procedures and internal registers, supported by trained staff who understand their roles in assessing and containing a breach.

To support clarity and consistency in how incidents are handled, Council follows six core stages that guide our readiness and our approach to assessing, containing, managing and resolving a breach.

Council's internal data breach response plan outlines the actions that will be taken when a data breach occurs and provides a structured process to ensure incidents are managed effectively and responsibly.

Six Stages that Support Readiness, Response and Reporting. *Source: Office of the Information Commissioner.*



Stage 1: Preparation

Council will:

- Maintain this Policy, a Data Breach Response Plan, and Cyber Incident Response Plan and Data Breach Incident Response Playbook.
- Build organisational capability through training and simulations.
- Integrate data breach management with risk, ICT security and business continuity frameworks.

Stage 2: Identification

Council will:

- Recognise potential breaches from internal or external sources, including contractors, other agencies or the public.
- Triage and escalate potential data breaches promptly.
- Consider whether the incident could be an Eligible Data Breach involving personal information by assessing the data breach to make a preliminary assessment of the risk posed by the breach
- Coordinate response as required to ensure an effective and timely management of the breach.

Stage 3: Containment and mitigation

Council will:

- Take immediate reasonable steps to stop further unauthorised access or disclosure and to recover information where possible.
- Apply proportionate controls, for example suspending access, revoking credentials, isolating systems, recalling emails or contacting unintended recipients.
- Commence a preliminary risk appraisal covering information sensitivity, scale and potential impacts to individuals.

Stage 4: Assessment

Council will:

- Where there is a reasonable suspicion of an Eligible Data Breach, complete an assessment within 30 days to decide if there are reasonable grounds to believe the breach is eligible. Extensions may be used only as permitted by the IP Act.
- Consider statutory serious harm factors, document decisions and preserve evidence.
- Decide on any need to engage external forensic or legal expertise.

Stage 5: Notification

Council will:

- Notify the OIC and affected individuals as soon as practicable if Council knows or assesses the breach as an Eligible Data Breach and no exemption applies.
- Notify the OIC by written statement with required information.
- Appropriately notify individuals impacted by an Eligible Data Breach. If individual contact is not reasonably practicable, Council will publish required information on its website for at least 12 months and advise the OIC how to access the notice.

Stage 6: Post-incident review and remediation

Council will:

- Conduct a structured lessons-learned review, assign actions and track remediation to completion.
- Update practices, systems, training and contracts as required.
- Ensure a complete record of the incident and response is captured in line with obligations under the *Public Records Act 2023*.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Councillors, Council employees, volunteers, and contractors and contracted service providers handling Council information under service arrangements.	• Comply with the Data Breach Policy and understand what is expected of them. • Comply with the IP Act, including protecting personal information held by the Council 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 including your supervisor or manager, Information and Technology Services and/or the Information Governance Unit. • Respond to requests for information from and cooperate with the Privacy Officer and Information and Technology Services as required. • Comply with recordkeeping obligations.
Delegated Privacy Officer	• 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 Executive Manager Information and Technology Services and Director People and Organisational Performance. • 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 Council website under section 53(1)(c) of the IP Act. • Immediately report a data breach that is also a cyber security incident to the Executive Manager Information and Technology Services, if not already reported. • Maintain the Register of Eligible Data Breaches.
Supervisors and Managers	• Identify and escalate concerns within your area of responsibility that may trigger the requirements of this Data Breach Policy. • Immediately report a data breach that is also a cyber security incident to the Executive Manager Information and Technology Services, if not already reported.

Role	Responsibility
Executive Manager Information and Technology Services	• Immediately report a cyber security incident that is also a data breach to Council's Privacy Officer, if not already reported. • Implement the Cybersecurity Management Plan and related procedures if the data breach is also a cyber security incident. • Escalate matters to the Business Continuity Team (BCT), when appropriate.

RELATED DOCUMENTS

Information Privacy General Policy
Information Security Management Administration Instruction
Data Breach Response Plan

◆◆◆◆◆◆

This policy is to remain in force until otherwise determined by Council.

Director responsible for Review: **Director People and Organisational Performance**

ORIGINALLY ADOPTED: {Enter Date}
CURRENT ADOPTION: {Enter Date}
DUE FOR REVISION: {Enter Date}
REVOKED/SUPERSEDED: {Enter Date}

.....
Ken Gouldthorp
CHIEF EXECUTIVE OFFICER