INFORMATION BREACH POLICY

POLICY STATEMENT

The City of Kalgoorlie-Boulder is committed to protecting the information it collects, stores and manages in the course of delivering its services. The City recognises that information breaches may occur due to human error, system failures, malicious activity or other circumstances. This policy establishes the City's approach to identifying, responding to and managing information breaches in a timely, consistent and transparent manner whilst maintaining compliance with the Privacy and Responsible Information Sharing Act 2024 (WA).

PURPOSE

The purpose of this policy is to:

- Outline the City's approach to managing information breaches
- Minimise harm to individuals and the organisation in the event of an information breach
- Supports compliance with legislative and regulatory obligations in relation to information breaches
- Reinforces accountability and transparency in information handling
- Ensure timely reporting and escalation to minimise impact and reoccurrence
- Provide a framework for consistent and coordinated responses to information breaches

SCOPE

This policy applies to:

- All City employees
- Contractors and consultants
- Volunteers and temporary staff
- Elected members
- Any other persons who access or manage information on behalf of the City

This policy applies to all information held by the City, including, but not limited to:

- Personal and sensitive personal information
- Corporate information
- Information in digital and physical formats
- All systems, services and records in the organisation

Document Set ID: 4162068
Version: 1, Version Date: 25/06/2026

DEFINITIONS

Corporate information means Information that supports the administration, governance and management of the organisation, including records relating to finance, human resources, legal matters, policy development and strategic planning.

Confirmed information breach means an information breach that has been verified through investigation or evidence.

Information Breach means unauthorised access to, disclosure of or loss of information held by the City.

Information Classification means the process of categorising information based on its sensitivity, value and level of risk, to ensure it is appropriately protected, handled and managed throughout its lifecycle.

Notifiable Information Breach means a breach involving personal information where unauthorised access, disclosures or loss is likely to result in serious harm to an individual. In certain circumstances, this type of breach may require notification to affected individuals and/or relevant regulatory authorities in accordance with applicable legislation.

Operational information means information created or used in the delivery of the City's services, programs and day-to-day business activities, including records relating to customer interactions, service delivery, projects and regulatory functions.

Personal Information means information or an opinion about an identified individual or an individual who is reasonably identifiable.

Sensitive Personal Information means personal information that is more sensitive in nature and requires a higher level of protection. This includes information such as health, genetic or biometric data, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, trade union membership or criminal record.

Shared Information Breach means an information breach involving information that has been shared with, or received from, another organisation or entity, where that information is accessed, disclosed or lost without authorisation.

Suspected information breach means a situation where there are reasonable grounds to believe that information may have been accessed, disclosed or lost without authorisation, but this has not yet been confirmed.

POLICY DETAILS

The City will manage information breaches in accordance with the following principles:

Document Set ID: 4162068
Version: 1, Version Date: 25/06/2026

1. **Definition and Identification**
   The City will clearly define what constitutes an information breach and support staff in recognising and reporting potential incidents.

2. **Assessment, Containment, Mitigation**
   The City will take reasonable steps to contain breaches, assess risks and impacts, and mitigate potential harm to individuals and the organisation.

3. **Preparedness**
   The City will maintain appropriate governance, systems, processes and training to prevent and respond to information breaches. This includes promoting staff awareness and ensuring clear reporting pathways are in place.

4. **Meeting Obligations**
   The City will meet applicable legal, regulatory and contractual obligations when responding to an information breach, including engagement with relevant authorities where required.

5. **Roles and Responsibilities**
   The City will maintain clear accountability for the management and oversight of information breaches.

6. **Record Keeping**
   The City will document suspected and confirmed information breaches, including actions taken and outcomes, to support accountability and continuous improvement.

7. **Review and Improvement**
   The City will review information breaches to identify lessons learned and strengthen controls, processes and practices.

REPORTING INFORMATION BREACHES

All employees, contractors, elected members and other relevant personnel must immediately report any suspected or confirmed information breach to their manager and the City's Privacy Officer.

An information breach may occur where information is accessed, disclosed or lost without authorisation.

Examples of information breaches may include, but not limited to:

- Sending information to the wrong recipient
- Unauthorised access to systems or records
- Loss or theft of devices containing information

Document Set ID: 4162068
Version: 1, Version Date: 25/06/2026

- Accidental publication or disclosure of information
- Cyber security incidents that result in information exposure.

Failure to report a suspected information breach may increase the potential harm to individuals and the organisation.

MANAGEMENT OF INFORMATION BREACHES

The City will respond to information breaches in a timely and proportionate manner. At a high level, this includes:

- Identifying and evaluating the breach
- Containing the breach to prevent further impact
- Assessing risks and potential harm
- Taking appropriate steps to mitigate impacts
- Determining whether external notification is required
- Reviewing the incident to inform improvements

Detailed procedures for managing information breaches are outlined in the Information Breach Response Plan.

RISK AND IMPACT MANAGEMENT

Each information breach will be assessed to determine the likelihood and consequences.

The City will manage risks in accordance with its Risk Management Framework, including escalation to the Executive Leadership Team and Audit Risk and Improvement Committee where required.

INFORMATION BREACH REGISTER

The City will maintain an Information Breach Register to record suspected and confirmed breaches.

The register will include:

- The nature of the breach
- How the breach occurred
- Actions taken to contain and mitigate the breach
- Whether individuals or external parties were notified
- Corrective actions implemented

The register supports monitoring, reporting and continuous improvement.

The register will be reported to external bodies as required under legislation.

Document Set ID: 4162068
Version: 1, Version Date: 25/06/2026

EXTERNAL REPORTING AND NOTIFICATION

In certain circumstances, the City may be required to notify external authorities or organisations of an information breach.

This may include regulatory bodies, law enforcement agencies or other relevant entities, depending on the nature and severity of the breach.

Decisions regarding external notification will be made in accordance with applicable legislation, contractual obligations and the City's governance processes.

ROLES AND RESPONSIBILITIES

Role	Responsibilities
Elected Members	Must handle information in accordance with this policy and relevant legislation, maintain confidentiality of information obtained through their role and report any suspected or confirmed information breaches.
Chief Executive Officer	Responsible for ensuring the City complies with relevant legislation and maintains appropriate governance arrangements for the management of information breaches.
Directors	Responsible for ensuring appropriate governance, oversight and controls are implemented within their directorates to support the prevention and management of information breaches.
Managers	Responsible for ensuring employees within their areas understand and comply with this policy and promptly report suspected or confirmed information breaches. Managers are also responsible for supporting breach response activities where required.
Privacy Officer	Responsible for overseeing the management of information breaches, including assessment, coordination of response activities, notification requirements and maintenance of the Information Breach Register.
Information Management	Responsible for supporting the coordination, investigation, documentation and recordkeeping requirements relating to information breaches and maintaining the Information Breach Register.
Information Technology (ICT)	Responsible for assisting with the identification, containment, investigation and remediation of technical or cyber-related information breaches.

Document Set ID: 4162068
Version: 1, Version Date: 25/06/2026

Role	Responsibilities
Employees, Contractors and Other Personnel	Responsible for handling information appropriately, complying with this policy and related procedures and immediately reporting suspected or confirmed information breaches.

TRAINING AND AWARENESS

The City will provide ongoing training and awareness to ensure staff understand their responsibilities in preventing, identifying and responding to information breaches.

RELATED DOCUMENTS

This policy should be read in conjunction with:

- Information Breach Response Plan
- Information Breach Register
- Privacy Policy
- Records Management Policy
- Cyber Security Incident Management and Response Plan

COMPLIANCE REQUIREMENTS

This policy supports compliance with:

- Privacy and Responsible Information Sharing Act 2024 (WA)
- State Records Act 2000 (WA)
- Local Government Act 1995 (WA)
- Information Privacy Principles (IPP)
- Australian Signals Directorate (ASD)
- Any other relevant legislation and regulatory requirements

REVIEW

This policy will be reviewed annually, or following a significant information breach, to ensure it remains current and effective.

DOCUMENT CONTROL				
Responsible Department	Information Management			
Description of Changes				
Version	Resolution Number	Endorsement Date:	Last Reviewed Date:	Next Review Date:
1	15.3.2.2	15 June 2026	May 2026	May 2027