Council Policy

Information Breach

Legislation/local law requirements:	*State Records Act 2000* *Local government Act 1995* *Freedom of Information Act 1992* *Privacy and Responsible Information Sharing Act 2024*
Relevant Delegation:	Refer to the City's delegation register.
Related policy procedures and documents	*Privacy Policy* *Recordkeeping Plan* Recordkeeping guidelines and procedures *FOI Statement* *Breach Register (internal)* *Security Risk Assessment (SRA) methodology* *PIA Register* *Privacy Impact Assessment Guide* *Privacy Impact Assessment (PIA) Template*

Introduction

The City of Kwinana (City) is committed to ensuring that personal information it receives is collected and handled in a manner that protects individuals' privacy.

This Information Breach Policy (Policy) sets out the City's approach to identifying, managing, and responding to actual or suspected data breaches to minimise harm and uphold privacy rights. The Policy aligns with the *Privacy and Responsible Information Sharing Act 2024* (Act) (including the Information Privacy Principles (IPPs)). By ensuring a timely and effective response, the City aims to safeguard community trust and comply with its legal obligations in the event of an information breach.

Purpose

The purpose of this Policy is to explain, in a clear and transparent manner, the following:

- What constitutes an information breach;
- How the City identifies, reports, and responds to an actual or suspected breach;
- Who must be notified in the event of a breach;
- The measures in place to prevent and mitigate information breaches;
- The rights and responsibilities of individuals affected by a breach; and
- How breach response is recorded and governed (including an internal Breach Register and post-incident reviews).

Objective

The objectives are to:

- Comply with the Act and other relevant legislation;
- Protect the personal and health information held by the City from unauthorised access, disclosure, or loss;
- Respond swiftly and effectively to actual or suspected information breaches to minimise harm;
- Ensure transparency in how the City manages and mitigates information breaches;

- Maintain public trust and confidence by upholding the highest standards of information security and privacy protection; and
- Support responsible information sharing by ensuring any disclosure during incident response is necessary, proportionate, limited to the minimum required, and safeguarded.

Scope

This Information Breach Policy applies to all instances of actual or suspected information breaches involving personal or health information held by the City, regardless of how the information is stored or collected. This includes breaches related to:

- Digital systems, databases, and online services managed by the City;
- Physical records and documents containing personal or health information;
- Emails, phone communications, and in-person interactions where sensitive information is exchanged; and
- Third-party service providers handling information on behalf of the City.

This Policy does not apply to information that is demonstrably de-identified such that individuals cannot reasonably be re-identified. Where a re-identification risk exists, the Policy applies.

Policy Provisions

Definitions

'Information breach' means any incident where personal or sensitive information is accessed, disclosed, lost, or stolen without proper authorisation. This includes unauthorised access to or sharing of data, accidental exposure, or any situation where the confidentiality, integrity, or security of the information is compromised, potentially putting individuals at risk of harm.

'Personal information' is information which relates to individuals and includes any information or opinion about them. It can include a name, address, phone number, email address or any information from which a person's identity can be reasonably ascertained.

'**Notifiable information breach'** means an information breach that is reasonably likely to result in a serious risk of harm to one or more individuals to whom the information related, having regard to the sensitivity of the information, circumstances of the breach and any mitigation actions taken. A notifiable information breach also includes any circumstances prescribed in a notifiable information breach determination made under section 60 of the Act.

Policy Statement

The City is committed to protecting personal and health information by ensuring a proactive, timely and effective response to actual or suspected information breaches. This policy outlines the City's responsibilities in identifying, managing, and mitigating breaches.

An information breach may occur in various circumstances, including but not limited to:

- Unauthorised access, loss, or theft of personal or health information held by the City;
- Accidental disclosure of information through correspondence, emails, or system errors;
- Cybersecurity incidents affecting City-managed platforms and services, including the 'Love My Kwinana' engagement hub;
- Misuse or mishandling of information collected through event registrations, applications or community consultations; and
- Data breaches involving third-party service providers engaged by the City.

The City will take immediate and appropriate action to investigate breaches, minimise risks, and protect affected individuals while ensuring compliance with legal and regulatory requirements.

Contracted service providers (CSPs) handling personal information must promptly notify the City on becoming aware of a suspected breach, preserve relevant evidence, cooperate with investigations, and comply with applicable privacy and security obligations.

Definition of an Information Breach

An information breach occurs when there is:

- unauthorised access to or disclosure of personal or health information;
- loss, theft, or destruction of personal or health information; or
- a breach of confidentiality that exposes personal or health information to unauthorised parties.

Examples of information breaches include:

- accidental sending of personal information to the wrong recipient;
- loss of a laptop or device containing sensitive information; or
- unauthorised access to personal data by employees or third parties.

Roles and Responsibilities

To ensure an effective response to information breaches, the following roles and responsibilities have been established within the City:

- City Employees and Contractors: Responsible for following all security protocols, promptly reporting any suspected breaches, and fully cooperating with investigations to resolve the issues;
- Information Security Officer / Privacy Officer: Oversee the coordination of the response to any information breaches, manage the investigation process, and ensure that the relevant authorities are notified as required by law; and
- Executive Management: Accountable for ensuring the effective implementation of this policy, supporting the necessary resources for breach management, and ensuring compliance with all privacy and security obligations.

Identifying and Reporting an Information Breach

Employees and contractors must immediately report any actual or suspected information breach to the Information Security Officer or designated Privacy Officer. Suspected breaches may be identified through:

- Routine audits or monitoring activities;
- Reports from staff or individuals affected by a breach; and
- External alerts (e.g., cybersecurity notifications).

Reports should include the following information:

- Nature of the breach;
- The date and time the breach was identified;
- The type of information involved;
- The potential risks associated with the breach; and
- Any initial containment actions taken.

Responding to an Information Breach

Upon identifying a breach, the City will:

- Assess the severity, scope, and potential harm of the breach;
- Contain the breach to prevent further unauthorised access or disclosure (e.g disabling compromised systems, securing physical records);
- Investigate the cause of the breach and identify any parties responsible for the incident; and
- Document all steps taken in response to the breach, including mitigation efforts and communications.

Assessment and Reporting Timeframe

The City will assess all suspected information breaches as soon as practicable but, in any case, within 30 days after becoming aware of the breach to determine whether a notifiable information breach has occurred.

The assessment will consider:

- The nature and severity of the information involved;
- The circumstances of the breach;
- The likelihood of serious harm to affected individuals; and
- Any actions taken to reduce the risk of harm.

Notifying Affected Individuals and Authorities

Where the City determines that a notifiable information breach has occurred, the City will notify affected individuals and the Western Australian Information Commissioner as soon as practicable after completing its assessment.

Notifications to individuals will include, at a minimum:

- a description of the breach;
- the type of information involved;
- the likely risks of harm;
- steps taken by the City to mitigate harm;
- recommended steps individuals can take; and
- a City contact point for further information.

Where individual notification is not reasonably practicable, the City will publish a public notification available for a period of 12 months in accordance with section 63(3) of the Act.

Exceptions to Notification

The City may not be required to notify affected individuals in certain circumstances, including:

- When notification would pose a serious risk to information security, public safety, or law enforcement efforts;
- When remedial actions have been taken to eliminate the risk of harm to affected individuals; or
- When the breach involved de-identified or encrypted data, making it unlikely that individuals will suffer harm.

Where the City determines that notification to affected individuals is not required under the Act, the City will:

- document the reasons for the decision;
- record the mitigation measures implemented; and
- provide a written notice to the Western Australian Information Commissioner outlining the basis for the decision.

Decisions will be approved by the relevant officers.

Information Commissioner's Powers

The Western Australian Information Commissioner has the authority to oversee the City's compliance with information breach assessment and notification requirements. If the Commissioner suspects that a notifiable information breach has occurred, they may direct the City to:

- Conduct a formal assessment of the suspected breach within a specified timeframe;
- Notify affected individuals if it is determined that the breach poses a significant risk of harm; and
- Take necessary corrective actions to prevent further breaches and mitigate potential risks.

The City will fully cooperate with any directions issued by the Commissioner and ensure compliance with all legal obligations regarding privacy and data protection.

Prevention and Risk Mitigation Strategies

To prevent information breaches, the City will:

- Implement data security measures including encryption, firewalls, and access control systems;
- Conduct regular staff training on privacy and data protection policies;
- Perform cybersecurity audits and risk assessments; and
- Ensure all third-party service providers comply with relevant data protection standards.

Record-Keeping and Documentation

The City will maintain accurate records of all information breaches, including:

- Details of the breach (nature, scope, and risks);
- Actions taken in response to the breach;
- Correspondence with affected individuals and regulatory bodies; and
- Investigation findings and outcomes.

Additionally, the City will establish and maintain a Register of Notifiable Information Breaches recording all suspected and confirmed breaches, including:

- The assessment outcome and notifiable decision
- Whether the Western Australian Information Commissioner was notified;
- Steps taken to contain the breach and mitigate harm;
- Any public notice publication; and
- Actions implemented to prevent future breaches.

A summary of assessed notifiable information breaches will be included in the City's Annual Report, ensuring transparency and accountability in how the City responds to and manages privacy risks.

Records relating to information breaches will be retained in accordance with the *State Records Act 2000* and will be made available to the Western Australian Information Commissioner upon request.

Testing and Continuous Improvement

The City will periodically test its information breach response arrangements through training, simulations or tabletop exercises to ensure staff readiness and continuous improvement of breach management processes.

Consequences of Non-Compliance

Employees and contractors who fail to comply with the procedures outlined in this policy may face disciplinary action, including potential termination of employment or contract. Non-compliance with the Act or other legislation may also result in legal penalties for individuals or the City.

Cross-border or External Hosting (Breach Context)

Where personal information relevant to a breach is stored or processed outside Western Australia or Australia, the City will identify data locations and parties involved, ensure lawful transfer and appropriate safeguards, and coordinate notifications consistent with applicable requirements while prioritising protection of affected individuals.

Integration with the IPPs

This Policy supports and aligns with the IPPs under the Act, including:

- IPP 1–2 (Collection/Openness): transparent communications about breaches;
- IPP 3–4 (Use/Disclosure and Security): minimum necessary disclosure and robust security;
- IPP 5–6 (Access and Correction): enabling individuals to seek information and assistance; and
- IPP 7–10 (Data Quality, Identifiers, Accountability): maintaining accurate records, limiting identifiers, and ensuring auditable decisions.

OFFICER USE ONLY

Officers may amend this section without council approval.

Responsible Team	Information Management	
Initial Council adoption	Date: March 2026	Ref#: 61
Reviewed/amended	Date:	Ref#:
Next Review Date	Date: March 2028	
Policy Document Number	D25/12038	