Council Policy

Council Policy Name:	**Information Breach Policy**		
Responsible Directorate:	**Corporate Strategy and Performance**	**Version**	**Adopted**

1. PURPOSE

1.1. The purpose of this Policy is to outline how the City identifies, manages and responds to suspected or actual Information Breaches. Aligning with the Privacy and Responsible Information Sharing (PRIS) Act 2024, it supports accountability, and public trust in our information handling practices.

2. SCOPE

2.1. This Policy applies to:

a. all employees, contractors and service providers of the City; and
b. all suspected or actual Information Breaches involving Personal Information held by, or on behalf of the City.

3. DEFINITIONS

Term	Meaning
OIC	Office of the Information Commissioner (WA)
Notifiable Breach	A breach where there is Unauthorised Access to or Unauthorised Disclosure of Personal Information, or a loss of Personal Information, that the City holds that is likely to result in Serious Harm to one or more individuals, and the City has not been able to prevent the likely risk of serious harm with remedial action.
Personal Information	Personal Information means information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion; and includes information of the following kinds: (i) a name, date of birth or address; (ii) a unique identifier, online identifier or pseudonym; (iii) contact information; (iv) information that relates to an individual's location; (v) technical or behavioural information in relation to an individual's activities, preferences or identity; (vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information; information that relates to 1 or more features specific to the physical, physiological, genetic, mental,

	behavioural, economic, cultural or social identity of an individual.
Sensitive Personal Information	Sensitive Personal Information means Personal Information - (a) that relates to an individual's - (i) racial or ethnic origin; or (ii) gender identity, in a case where the individual's gender identity does not correspond with their designated sex at birth; or (iii) sexual orientation or practices; or (iv) political opinions; or (v) membership of a political association; or (vi) religious beliefs or affiliations; or (vii) philosophical beliefs; or (viii) membership of a professional or trade association; or (ix) membership of a trade union; or (x) criminal record; or (b) that is health information; or (c) that is genetic or genomic information (other than health information); or (d) that is biometric information; or (e) from which information of a kind referred to in any of paragraphs (a) to (d) can reasonably be inferred;
Serious Harm	Serious Harm occurs where a reasonable person would objectively conclude that an Information Breach is likely to result in real and significant adverse impacts to an individual, having regard to the nature of the information, the circumstances of the breach, and the likely consequences. Potential harm may include: • discrimination; • financial loss; • loss of confidentiality; • reputational damage; • risk to physical safety; or • identity theft or fraud.
Unauthorised Access	Access to Personal Information held by the City by a person or system that is not permitted to do so.
Unauthorised Disclosure	The intentional or unintentional release, sharing, or making available of Personal Information to a person or entity that is not authorised to receive it.
Unique Identifiers	Unique identifier means a number or other identifier assigned by an entity to an individual to uniquely identify that individual for the purposes of the operations of the entity; but does not include an identifier that consists only of the individual's name.

4. STRATEGIC CONTEXT

Strategic Theme	Objective
OPPORTUNITY	16: Provide effective governance and organisational leadership

5. POLICY STATEMENT

5.1. An Information Breach is when there is Unauthorised Access to, Unauthorised Disclosure of, or loss of Personal Information or Sensitive Personal Information.

5.2. An Information Breach may occur through a range of circumstances, including human error, system failure, malicious activity or physical security incidents. Examples of Information Breaches may include but are not limited to:
a. loss or theft of devices, documents or systems containing information;
b. Unauthorised Access to information due to inappropriate access controls;
c. data loss resulting from equipment or system failure;
d. disclosure of information to an unintended recipient;
e. cyber security incidents such as phishing, hacking or malware attacks.

5.3. A suspected or actual Information Breach should be reported to the Privacy Officer as soon as practicable and in cases within 24 hours.

5.4. If an Information Breach is suspected or identified, the City will take all reasonable steps to:
a. contain the Information Breach as soon as reasonably possible and prevent further unauthorised access, disclosure or loss;
b. assess the nature and potential impact of the breach;
c. mitigate harm to individuals, the City and other affected parties; and
d. meet any applicable legal, regulatory, contractual and reporting obligations;

5.5. The City will assess whether an Information Breach is likely to result in Serious Harm to an individual. In the event of a Notifiable Breach, the City will notify the OIC in accordance with the PRIS Act 2024.

5.6. If information from another agency or third party is involved in an Information Breach, the City will consult with the relevant party to coordinate response actions.

5.7. Where required, the City's CEO may establish an Information Breach response team to manage the incident.

5.8. Information management, privacy and security practices will be regularly reviewed and improved to prevent Information Breaches and identify suspected or actual Information Breaches in a timely manner.

6. RELATED DOCUMENTATION / LEGISLATION

6.1. Privacy and Responsible Information Sharing (PRIS) Act 2024
6.2. Privacy Policy

7. REVIEW DETAILS

Review Frequency		3-yearly		
Council Adoption	**DATE**	27 May 2026	**Resolution #**	C2605/151
Previous Adoption	**DATE**		**Resolution #**	