Administration Policy

Personal Information Breach – Privacy and Responsible Information Sharing (PRIS)

fremantle.wa.gov.au

Personal Information Breach (PRIS)

Policy scope

This policy sets out how the City of Fremantle manages personal information breaches, in accordance with Section 73 of the *Privacy and Responsible Information Sharing Act 2024* (the PRIS Act).

This policy is to be read in conjunction with the City's Privacy Policy, the PRIS Act, and other relevant legislation.

Policy statement

The City of Fremantle (the City) is committed to protecting personal information and managing any personal information breaches effectively, in accordance with the PRIS Act.

This Policy establishes the procedures which the City will implement to:

- prevent personal information breaches;
- ensure timely identification, assessment, and response; and
- meet obligations under the PRIS Act, including notifiable personal information breach requirements.

1. Roles and responsibilities

1.1 All City employees, contractors and volunteers must:

1.1.1 comply with this policy and the City's Privacy Policy; and

1.1.2 report suspected or actual breaches immediately.

1.2 The City's Privacy Officer must:

1.2.1 coordinate breach responses, assessments, and notifications;

1.2.2 maintain a personal information breach register; and

1.2.3 provide regular relevant training to employees and Elected Members.

2. Personal information breach management process

2.1 The City will comply with the following process if a personal information breach is suspected:

1: Identify

All suspected breaches must be reported via the IT Service Desk (internal) or Customer Portal (external) immediately. Alternatively, suspected breaches can be reported in writing to governance@fremantle.wa.gov.au or PO Box 807, Fremantle WA 6959.

Commented [KH1]: Is there an alternative to customer portal for customers? Report to customer service for assistance?

A breach may include (but is not limited to):

- lost or stolen devices
- unauthorised system access
- accidental disclosure (e.g. email error)
- unlawful disclosure (e.g. intentional disclosure)

2: Contain

The Privacy Officer, must take reasonable steps to:

a. isolate affected systems;
b. recover and secure information; and
c. disable access.

The Privacy Officer must take reasonable steps to mitigate any harm caused by a suspected notifiable information breach within 30 days of the City becoming aware.

The City's IT department will assist the Privacy Officer with these steps.

3: Assess

The Privacy Officer, must determine:

a. what information is involved;
b. who is affected;
c. likelihood of harm; and
d. whether the breach is notifiable.

Within 30 days, the Privacy Officer must determine whether a notifiable breach has occurred, or whether there are reasonable grounds to believe that one has occurred, and to document the outcome of this assessment in a written report.

The Privacy Officer must consider any relevant privacy guidelines issued by authority bodies when assessing suspected notifiable personal information breaches.

4: Notify

Where is it determined that no breach has occurred, the individual or entity that reported the suspected breach is to be notified of the City's assessment outcome.

Where a notifiable information breach is confirmed, the Privacy Officer must:

a. notify the Information Commissioner in accordance with section 62 of the PRIS Act;
b. notify affected individuals as soon as practicable in accordance with section 63 of the PRIS Act; and
c. for assessed shared agency breaches, notify the relevant entity and Chief Data Officer of WA.

The City, in accordance with section 67 of the PRIS Act, is not required to notify affected individuals if the City reasonably believes that doing so would result in:

a. a serious threat to the life, health, safety or welfare of any individual; or
b. a threat to the life, health, safety or welfare of any individual due to family violence.

The City, in accordance with section 68 of the PRIS Act is not required to notify affected individuals if the City reasonably believes that doing so would:

a. have a material adverse effect on the security of personal information held by the City; or
b. be likely to lead to further information breaches in relation to personal information held by the City.

If section 67 and 68 of the PRIS Act applies, the City must notify the Information Commissioner accordingly (s 69).

5: Review and prevent

The Privacy Officer, must:

a. identify root causes;
b. implement corrective actions;
c. update procedures and provide training accordingly; and
d. comply with a direction given by the Information Commissioner, if any.

3. Personal information breach register and reporting

3.1 The City will maintain an internal register of all breaches.

3.2 The City will record all actions taken and outcomes in its record management system and the Personal Information Breach Register.

3.3 The City will report breaches as part of the Annual Report process (s 75).

4. Training and awareness

4.1 The City will provide appropriate training and information to employees and Elected Members in relation to their privacy responsibilities.

4.2 The City will ensure contractors and volunteers are aware of their requirement to comply with the Privacy Policy.

4.3 Non-compliance will be dealt with under the City's Code of Conduct.

Definitions and abbreviations

"Information breach" means unauthorised access to, or unauthorised disclosure of, information or loss of information.

"Notifiable Information Breach" *is a breach where:*

- unauthorised access/disclosure or loss occurs; and
- a reasonable person would conclude it is likely to result in serious harm.

"Serious Harm" includes physical, psychological, financial, or reputational harm. The following matters must be taken into account –

a. the nature of the information;
b. the sensitivity of the information;
c. whether the information is or was protected by security measures;
d. the persons, or the kinds of persons, who have obtained, or could obtain, the information;
e. the likelihood that the persons referred to in paragraph (d) —
   i. have or had the intention of causing harm; or
   ii. could or did circumvent security measures protecting the information;
f. the nature of the harm that has resulted or could result from the access, disclosure or loss;
g. any matters set out in PRIS privacy guidelines; and
h. any other relevant matters.

"PRIS Act" means the *Privacy and Responsible Information Sharing Act 2024*

"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.

This includes the following types of information:

- a name, date of birth or address
- a unique identifier, online identifier or pseudonym
- contact information
- information that relates to an individual's location
- technical or behavioural information in relation to an individual's activities, preferences or identity
- 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 one or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual.

Sensitive personal information includes information that relates to an individual's:

- racial or ethnic origin
- gender identity
- sexual orientation or practices
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- criminal record
- health information
- genetic or genomic information
- biometric information.

Responsibility and review information	
Responsible officer	Manager Governance and Manager Information and Technology
Document adoption/approval details	1 July 2026 - CEO - 6361031 *Council noted that the Information Breach Policy will be an Administration Policy approved by the CEO on 24 June 2026 (ARIC2606-2).
Document amendment details	Amendment approval/adoption date Proof of adoption/approval - meeting name or document no#
Next review date	1 July 2030 (maximum of four years from last review)