Information Handling and Breach Policy

Aligned City Value/s	**Approachable**	**Responsive**	**Transparent**
Responsible Directorate	**The Office of the CEO**		
Responsible Business Unit/s	**Governance and Corporate Information Services**		
Responsible Officers	**Manager Governance and Chief Technology Officer**		
Affected Business Unit/s	**All Business Units**		

Objective

The City values the privacy of its customers and stakeholders and takes reasonable steps to protect the information it handles from misuse and loss and from unauthorised access, modification, or disclosure. The City is committed to full compliance with the obligations and requirements of the proposed legislation regarding privacy and responsible information sharing ('PRIS').

The purpose of this Policy is to facilitate lawful and appropriate information handling by the City. The Policy also outlines the requirements to manage and respond to an information breach and to mitigate future breaches.

Scope

This Policy applies to Elected Members, all employees, contractors and volunteers undertaking duties on behalf of the City.

This Policy applies to all information handled by the City. Including, information regarding customers and stakeholders of the City, employees, contractors, volunteers, Elected Members and Committee Members.

Policy

INFORMATION HANDLING

The Collection of Personal Information

The City collects personal information about its customers and stakeholders in the performance of its functions and activities. Sensitive personal information is not collected, unless:

- It is necessary for the performance of one or more of the City's functions and activities; and
- The individual consents to the collection; or
- It is required or authorised by or under law; or
- It is necessary for the establishment, exercise or defence of a legal or equitable claim; or
- It is necessary for research, or the compilation or analysis of statistics, relevant to government-funded targeted welfare or educational services; or
- If the use or disclosure is necessary to prevent or lessen:
    - a serious threat to the life, health, safety or welfare of any individual; or
    - a serious threat to public health, public safety or public welfare; or
    - a threat to the life, health, safety or welfare of any individual due to family violence.

Access and Correction of Personal Information

In most circumstances, if an individual requests for their personal information to be updated, the City will update this outside of a formal process. Further, in circumstances where the individual requests access to their own personal information (i.e.: correspondence sent to/ from them, applications lodged by them), this is released to that individual outside of a formal process.

Under the *Freedom of Information Act 1992* (WA), a person has rights to access, correct and protect their personal information. Visit the City's Freedom of Information webpage for further information.

A person may also make requests for access to, and correction of, personal information to which Information Privacy Principle 6 applies, under the proposed PRIS legislation.

Disclosure of Information to Third Parties

The City may disclose customer and stakeholder information to third parties in the following circumstances:

- Under an information sharing agreement or information sharing request, with another public entity.
- With the consent of the customer or stakeholder;
- Where the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;
- As required or authorised by law or in response to a request from an investigative authority;
- If the use or disclosure is necessary for a law enforcement function to be performed by a law enforcement agency;
- To complete the purpose or function for which the information was provided;
- To improve the purpose or function for which the information was provided;
- If the use or disclosure is necessary to prevent or lessen:
    - a serious threat to the life, health, safety or welfare of any individual; or
    - a serious threat to public health, public safety or public welfare; or
    - a threat to the life, health, safety or welfare of any individual due to family violence.
- If it believes on reasonable grounds that non-compliance with the proposed PRIS legislation is necessary for the purposes of its, or any other entity's, child protection functions.
- If the information relates to family violence or alleged family violence and the individual to whom the collected information relates is the perpetrator, or alleged perpetrator, of the family violence.

The Protection of Information

The City is committed to safeguarding information against misuse, loss, modification and unauthorised access or disclosure.

The City will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose, unless required or authorised to retain the information by another law.

Multiple controls are implemented to protect information including encryption, multifactor authentication, security awareness training campaigns, endpoint security, email security, domain security, network security, third party risk assessments and other recommended controls defined in the Australian Signals Directorate Essential 8 Maturity level 1.

RESPONDING TO INTERFERENCES WITH PRIVACY

The City's designated Privacy Officer (the City's Legal and Integrity Officer) can be contacted regarding complaints made directly to the City in relation to acts or practices of the City that may constitute an interference with the privacy of an individual.

The Privacy Officer will then coordinate the responses to these complaints. The Privacy Officer can be contacted on corporatecompliance@stirling.wa.gov.au and (08) 9205 8555. The Privacy Officer will aim to provide the complainant with a formal response as soon as practicable, upon receiving all required information. Complainants will be advised of any unavoidable delay.

An interference with the privacy of individual/s, may also amount to an information breach. Information breaches include unauthorised access to, or unauthorised disclosure of, information or loss of information.

In the event of an alleged interference with privacy, a person may complain to the Information Commissioner of WA. It is the duty of the Information Commissioner, and members of Commissioner staff, to assist an individual who wishes to make a privacy complaint and requires assistance to formulate the complaint.

RESPONDING TO INFORMATION BREACHES

All complaints made are treated seriously and in accordance with the proposed PRIS legislation. The below sets out the process of responding to information breaches:

Complaints Process	Information Breaches
Reporting	Incidents related to information breaches must be reported immediately to the City's Privacy Officer and the Corporate Information Services ('CIS') Business Unit, on the below: CIS: servicedeskplus@stirling.wa.gov.au; cybersecurity@stirling.wa.gov.au Privacy Officer: corporatecompliance@stirling.wa.gov.au Any breach that relates to a suspected misconduct must also be reported in accordance with the City's Codes of Conduct.
Contain	All City officers must take reasonable steps to contain the suspected notifiable information breach. This obligation is ongoing as other steps proceed.
Initial Assessment	Within 2 business days, the City will make an initial assessment as to whether there is a reasonable suspicion that a notifiable breach has occurred. If so, the City will notify the affected people and regulator as soon as possible and commence a formal assessment.
Assessment	Within 30 days, determine whether or not a notifiable information breach has occurred or there are reasonable grounds to believe it has occurred and prepare a written report on the assessment.
Notification	Notification to the Information Commissioner of WA, must be made as soon as possible after the assessment. For assessed shared agency breaches, notification must also be sent to the Chief Data Officer of WA. The City will take all reasonable steps to give written notice of an assessed notifiable information breach to each affected individual or publish a written notice of the breach.
Post-Incident Review	A post incident review will consider: • All reasonable steps to mitigate any harm caused by the notifiable information breach; • The steps to be taken to prevent similar future breaches or mitigate the identified risk; • A cause analysis of the breach; • Security audit of both physical, technical and cyber security controls; • Review of employee training practices;

Complaints Process	Information Breaches
	• Review of contractual obligations with contracted service providers; • Any other review considerations, recommendations or guidelines published by the Information Commissioner of WA or the Chief Data Officer of WA.

Roles and Responsibilities

The below sets out the roles and responsibilities of key stakeholders of the City in relation to information breaches.

Roles and Responsibilities	
All Employees, Contractors, Volunteers and Elected Members	• Ensuring that they are familiar with City's PRIS obligations and how they apply to their work. • Immediately reporting or referring information breaches or identified privacy risks.
The Cyber-Security Incident Response Team	• This team is enacted in accordance with the City's Crisis Communications Framework. • Responsible for containing, remediating and recovering the services after the incident.
The Privacy Officer (the Legal and Integrity Officer)	• Promotes the City's compliance with the incoming information privacy principles ('IPP'). • Assists in the conduct of privacy impact assessments by the City. • Coordinates the City's response to complaints, in relation to acts or practices of the City that may constitute an interference with the privacy of an individual. Including, privacy interferences that may also be constituted as an information breach • Coordinates the City's dealings with the Information Commissioner. • Will refer any information breaches that relate to suspected employee or Elected Member misconduct to the City's Integrity Panel, for consideration.
The Information Sharing Officer (the Coordinator Information Management)	• Coordinates the City's dealings with the Chief Data Officer of WA. • Coordinates Information sharing requests made by or to the City; • Coordinates Information sharing agreements entered into or proposed to be entered into by the City. • Assists in the conduct by the City of the following assessments: - Assessments of the responsible sharing principles. - Privacy impact assessments. • Aboriginal information assessments.
The Audit Committee	• Maintains oversight of Artificial Intelligence risks and any information breaches through the Accountable Stirling Quarterly Report.
The Crisis Management Team ('CMT') (the Executive Team)	• Foster a culture and values that ensures privacy is embedded in the work environment. • Ensure that any privacy impact associated with new initiatives is assessed and steps are taken to mitigate privacy risks. • Provide senior management of information breach incidents.
External Reporting	• People may contact the Information Commissioner of WA regarding interferences with privacy and information breaches. • People may contact the Chief Data Officer of WA regarding assessed shared information breaches.

Definitions

Handle, in relation to information, means to collect, hold, manage, use or disclose the information.

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

Interference with Privacy includes:

a) acts done, or practice engaged in, by the City in contravention of the proposed *Privacy and Responsible Information Sharing Act 2024* (WA)('the PRIS Act'), in relation to personal information or de-identified information that relates to an individual.
b) A failure by the City to comply in relation to its obligations under the PRIS Act, relating to suspected or assessed notifiable information breaches, that involve personal information.
c) A failure to comply in relation to a function or activity involving the handling of personal information.

Notifiable Information Breach occurs in the below three circumstances:

1)
   a) There is unauthorised access to, or unauthorised disclosure of, personal information held by an IPP entity; and
   b) a reasonable person would conclude that the access or disclosure is likely to result in serious harm to any individual to whom the information relates.
2)
   a) If personal information held by an IPP entity is lost in circumstances in which unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
   b) If the access or disclosure of the information were to occur, a reasonable person would conclude that it would be likely to result in serious harm to any individual to whom the information relates.
3)
   a) If there is unauthorised access to, or unauthorised disclosure of, personal information held by an IPP entity; or
   b) personal information held by an IPP entity is lost; and
   c) the access, disclosure or loss occurs in circumstances set out in a notifiable information breach determination.

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:

a) a name, date of birth or address;
b) a unique identifier, online identifier or pseudonym;
c) contact information;
d) information that relates to an individual's location;
e) technical or behavioural information in relation to an individual's activities, preferences or identity;
f) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information;
g) 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 means personal information that relates to an individual's

a) racial or ethnic origin; or
b) gender identity, in a case where the individual's gender identity does not correspond with their designated sex at birth; or
c) sexual orientation or practices; or
d) political opinions; or
e) membership of a political association; or
f) religious beliefs or affiliations; or
g) philosophical beliefs; or

h) membership of a professional or trade association; or
i) membership of a trade union; or
j) criminal record; or
k) health information; or
l) genetic or genomic information; or
m) biometric information.

Relevant management practices/documents

City of Stirling Employee Code of Conduct
City of Stirling Council Members, Committee Members and Candidates Code of Conduct
Crisis Communications Framework
Cyber Security Incident Response Plan
Freedom of Information Statement
Information Management Policy
Information Security Management Practice
The City's Privacy Statement

Legislation/local law requirements

Freedom of Information Act 1992 (WA)

Freedom of Information Regulations 1993 (WA)

Proposed *Information Commissioner Act 2024* (WA)

Proposed *Privacy and Responsible Information Sharing Act 2024* (WA)

State Records Act 2000 (WA)

Office use only				
Relevant delegations				
Initial Council adoption	**Date**	17 September 2024	**Resolution #**	0924/009
Last reviewed	**Date**		**Resolution #**	
Next review due	**Date**	17 September 2026		