

CP.61 Privacy, Information Handling and Breach of Information

<i>Responsible Department</i>	Office of the Chief Executive Officer Corporate Services
<i>Resolution Number</i>	C.5334
<i>Resolution Date</i>	18/06/2025
<i>Next Scheduled Review</i>	2026/2027
<i>Related Shire Documents</i>	Council Policy CP.3 Code of Conduct for Councillors Committee Members and Candidates Management Policy MP.1 Code of Conduct – Employees, Volunteers, Contractors and Agency Staff Customer Service Charter Freedom of Information Statement Council Policy CP.56 Records Management Policy Council Plan 2022-2032, Outcome 12 Process - Manage Complaints - Information Breach Process – Manage Document Control Business Continuity Plan Process – Manage Records
<i>Related Legislation</i>	<i>Freedom of Information Act 1992</i> <i>Freedom of Information Regulations 1993 (WA)</i> <i>Local Government Act 1995, s.5.94 & s.5.95</i> <i>Local Government (Administration) Regulations 1996, Part 7</i> <i>Privacy Act 1988 (Cth)</i> <i>Privacy and Responsible Information Sharing Act 2024 (WA)</i> <i>Information Commissioner Act 2024 (WA)</i> <i>State Records Act 2000 (WA)</i>

OBJECTIVE

The objective of this policy is to ensure all reasonable steps are taken so that the collection, use, disclosure and handling of all Personal Information by the Shire of Northam (the Shire) aligns with relevant Australian Privacy Principles and the obligations and requirements of the legislation regarding privacy and responsible information sharing ('PRIS').

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

SCOPE

This policy applies to all Council Members and Employees of the Shire as well as to contracted third parties responsible for handling Personal and/or Sensitive Information held and managed by the Shire.

This Policy applies to all information handled by the Shire, including, information regarding customers and stakeholders of the Shire, employees, contractors, volunteers, Council Members and Committee Members.

POLICY

1. 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 Shire in contravention of the 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 Shire 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.

Information Privacy Principles (IPP) entity has the meaning given in the *Privacy and Responsible Information Sharing Act 2024*.

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 about an identified individual, or an individual who is reasonably identifiable:

- a) Whether the information or opinion is true or not; and
- b) Whether the information or opinion is recorded in a material form or not.

This includes information the Shire has collected such as data or information in any format including correspondence, in person, over the phone or over the Internet, or sourced from third parties.

Personal Information includes but is not limited to names, address, telephone numbers, email addresses, date of birth and rates records.

Personal Information does not include information about an individual that is contained in a publicly available publication as set out in the Local Government Act 1995. Personal Information, once it is contained in a publicly available publication, ceases to be covered by the Privacy Policy.

Sensitive Information means personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information.

2. Policy Statement

The Shire of Northam (the Shire) considers that the responsible handling of Personal Information is a key aspect of democratic governance and is committed to protecting an individual's right to privacy.

3. Implementation

All Managers within the Shire are responsible for the implementation of the policy within their Service Unit.

The Business Solutions Coordinator will monitor data governance in accordance with its policies and processes to ensure that Personal Information held by the Shire is protected from misuse, interference, loss, unauthorised access, modification or disclosure.

Reflecting the Australian Privacy Principles, specific policy commitments are made in respect of the different activities involved in the management of Personal Information.

3.1 Collection of Personal Information

- The Shire will only collect Personal Information that is reasonably necessary for, or directly related to, its obligations or performing one or more of the Shire's functions or activities as a local government.
- The Shire will only collect Personal Information by lawful and fair means.
- The Shire will not collect Sensitive Information about an individual without their consent.
- The Shire usually collects Personal Information directly from the individual concerned.
- The Shire will collect Personal Information from other parties if consent is given in writing by the individual or required by law.
- The Shire will notify the individual of the collection of Personal Information at, before or as soon as practicable after the collection of the information.
- The Shire website uses Google Analytics and cookies to help analyse how users use the Shire website. The Shire will never (and will not allow any third party to) use the statistical analytics tool to track or collect any personal information of visitors to the Shire's site. The Shire will not link, or seek to link, an IP address with the identity of a computer user. The Shire will not associate any data gathered from this site with any Personal Information from any source, unless the individual explicitly submits that information via a fill-in form on the Shire website.

3.2 Storage of Personal Information

- The Shire will store Personal Information in a range of mediums including electronic systems (onsite and in the cloud (in Australia and overseas)) or paper files.
- All information is stored securely, meets the requirements of legislation and best practice guidance and access is restricted to authorised personnel only in accordance with the Shire's Records Management Policy and Recordkeeping Plan.
- Where Personal Information is stored by a contracted third party, the Shire requires them to comply with this policy.

3.3 Use or Disclosure of Personal Information

- The Shire will only use or disclose Personal Information for the primary purposes for which it was collected or for directly related secondary purposes which would be reasonably expected by the individual, or as permitted or required by law. If there is any doubt about this expectation, then consent will be sought from the individual prior to disclosure of Personal Information for a secondary purpose.
- Where Personal Information is shared with a third party who is under contract with the Shire, the Shire will require them to comply with this policy.
- The Shire will not use Personal Information for an automated decision-making process.

3.4 Quality of Personal Information

- The Shire will take reasonable steps to ensure that the Personal Information is relevant, accurate and up-to-date before using it.
- The Shire will take steps, as reasonable in the circumstances to ensure that Personal Information it collects is relevant and not excessive.
- The Shire will update Personal Information held when necessary or when the individual concerned advises the Shire that their Personal Information has changed.

3.5 Security of Personal Information

- The Shire will take steps to protect Personal Information held by the Shire from misuse, interference, loss, unauthorised access, modification, or disclosure.
- The Shire has data protection and security measures including administrative, physical and technical access restrictions to Personal Information to ensure access by only authorised personnel.
- The Shire will ensure that Personal Information is not kept any longer than necessary or destroyed or de-identified in line with accepted document disposal schedules and the Shire's Recordkeeping Plan.
- The Shire will ensure that Personal Information which is transferred or stored outside of Australia will comply with ISO 27001 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

3.6 Responding to Interferences with Privacy

The Shire's designated Privacy Officer (Manager Governance and Risk or Governance Officer) can be contacted regarding complaints made directly to the Shire in relation to acts or practices of the Shire 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 records@northam.wa.gov.au or (08) 9622 6100. 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.

3.7 Responding to Information Breaches

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

<https://au.promapp.com/shireofnortham/Process/Minimode/Permalink/CqKePOnGCLROkk8JLcTmCi>

3.8 Other Agreements Relating to Data Privacy

The policy recognises that separate agreements, licences and memoranda of understanding may be entered into between the Shire and third parties such as State and Federal agencies, to govern access to and usage of specific data resources. Where this occurs, the Shire requires them to comply with this Policy.

3.9 Unique identifiers

Some of the unique identifiers that the Shire may collect include Medicare numbers, Tax File Numbers, Drivers Licence numbers and Australian Passport numbers.

3.10 De-identification of personal information

De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so e.g. removing personal and unique identifiers (name, address, date of birth or other recognisable characteristics).

3.11 Roles and responsibilities

The Business Solutions Coordinator and Manager Governance and Risk will be responsible for:

- The publication of and compliance with this policy.
- The development of supporting documentation and providing interpretations in the event of the need for clarification.

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

Roles and Responsibilities	
All Employees, Contractors, Volunteers and Council Members	<ul style="list-style-type: none"> Ensuring that they are familiar with Shire'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	<ul style="list-style-type: none"> This team is enacted in accordance with the Business Continuity Plan. Responsible for containing, remediating and recovering the services after the incident.
The Privacy Officer	<ul style="list-style-type: none"> Promotes the Shire's compliance with the incoming information privacy principles ('IPP'). Assists in the conduct of privacy impact assessments by the Shire. Coordinates the Shire's response to complaints, in relation to acts or practices of the Shire 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 Shire's dealings with the Information Commissioner. Will refer any information breaches that relate to suspected employee or Council Member misconduct to be handled in accordance with the Shire's policy.
Information Sharing Officer	<ul style="list-style-type: none"> Coordinates the Shire's dealings with the Chief Data Officer of WA. Coordinates Information sharing requests made by or to the Shire; Coordinates Information sharing agreements entered into or proposed to be entered into by the Shire. Assists in the conduct by the Shire of the following assessments: <ul style="list-style-type: none"> Assessments of the responsible sharing principles. Privacy impact assessments. Aboriginal information assessments.
Audit, Risk and Improvement Committee	<ul style="list-style-type: none"> Maintains oversight of privacy risks and any information breaches.
The Crisis Management Team ('CMT') as established by the Business Continuity Plan	<ul style="list-style-type: none"> 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.

3.12 Requesting access or correcting personal information

Subject to applicable laws and regulations, an individual may have some or all of the following rights with respect to their personal data:

- to access their personal data and to rectify any inaccuracies within that personal data;
- to request for the erasure of their personal data residing with the Shire;
- to request their personal data in portable, machine-readable format; and
- to withdraw their consent to the Shire's processing of their personal data.

An individual can contact the Shire with a request relating to the personal information the Shire holds about them by email at records@northam.wa.gov.au or phone at (08) 9622 6100, including their name and contact details. The Shire may need to verify an individual's identity before providing them with their personal information.

In some cases, the Shire may be unable to provide an individual with access to all of their personal information and where this occurs, the Shire will explain why. The Shire will deal with all requests for access to personal information within a reasonable timeframe.

3.13 Information Asset Register

The Shire will maintain an Information Asset Register (IAR) to assist it in assessing risks and managing information efficiently. The IAR will support:

- The identification of personal information and the application of privacy safeguards.
- Awareness of information that can be publicly released or disclosed to trusted third parties.
- Information classification and the use of appropriate security controls to protect, store and share information assets.

3.14 Review of the Privacy Policy

The Shire will ensure that this Policy is reviewed at least every two years, or more frequently as required.