

## Strategic Outcome Supported: 10.1 – Provide strategically focused, open and accountable governance

### OBJECTIVE

1. The objective of this policy is to establish the Shire's commitment to protecting information held by the Shire and to provide a framework for identifying, reporting, managing, recording and learning from information breaches.
2. The policy promotes transparency, accountability and responsible information management practices while supporting compliance with applicable legislative obligations and community expectations.

### SCOPE

3. This policy applies to:
  - a. Elected Members;
  - b. The Chief Executive Officer;
  - c. Employees;
  - d. Contractors and consultants engaged by the Shire;
  - e. Volunteers acting on behalf of the Shire; and
  - f. Covers all functions, services, programs, records, systems and activities involving the collection, storage, use, disclosure or management of personal information.

### DEFINITIONS

4. **Information Breach** means unauthorised access to, unauthorised disclosure, or loss of information.
5. **Information Breach Register** means the internal register maintained by the Shire to record suspected and confirmed information breaches and actions taken in response.
6. **Personal Information** includes name, date of birth, address, contact information, location information and unique identifiers that relate to someone's features or behaviours. It includes information about a deceased person and inferences made about people.
7. **PRIS Act** means the *Privacy and Responsible Information Sharing Act 2024 (WA)*.
8. **Privacy Officer** means the officer appointed by the Chief Executive Officer to coordinate privacy and information management responsibilities.
9. **Shared Information** means information shared between agencies or organisations under an authorised information sharing arrangement.
10. **Shire** means Shire of Donnybrook Balingup.

## POLICY STATEMENTS

### Commitment

11. The Shire is committed to the secure and responsible management of information and will take reasonable steps to:
  - a. Protect information from unauthorised access, disclosure, misuse, alteration or loss.
  - b. Promote a culture of privacy awareness and accountability.
  - c. Respond promptly and effectively to suspected or actual information breaches.
  - d. Minimise harm arising from information breaches.
  - e. Maintain records of information breaches and corrective actions.
  - f. Continuously improve information management practices.

### Reporting Information Breaches

12. Any person who becomes aware of a suspected or actual information breach involving Shire information must report the matter as soon as practicable to their Manager and the Privacy Officer.

### Information Breach Response

13. The Shire will manage information breaches using the principles of containment, assessment, mitigation and review and improvement.

### Containment

14. Action will be taken to prevent further access, disclosure or loss of information.

### Assessment

15. The Shire will assess:
  - a. what information has been affected;
  - b. how the breach occurred;
  - c. who may be affected;
  - d. the level of risk or harm; and
  - e. whether notification obligations may apply.

### Mitigation

16. Reasonable steps will be taken to reduce potential harm to affected individuals, the Shire and other stakeholders.

### Review and Improvement

17. Following an incident, the Shire will identify lessons learned and implement corrective actions to reduce the likelihood of future breaches.
18. The Shire will regularly review its privacy practices and governance arrangements to improve compliance with legislative requirements and recognised best practice.

## Information Breach Register

19. The Shire will maintain an Information Breach Register to record:
- suspected and confirmed breaches;
  - actions taken;
  - notifications made;
  - corrective actions;
  - lessons learned; and
  - outcomes of investigations.

## Training and Awareness

20. The Shire will provide training and awareness initiatives to support employees, contractors and Elected Members in preventing, identifying and responding to information breaches.

## External Parties

21. Where services are provided by contractors, consultants or service providers, the Shire will seek to ensure appropriate contractual arrangements are in place regarding information security and information breach reporting.

## Notifications

22. Where required, the Shire may notify:
- affected individuals;
  - regulators;
  - government agencies;
  - law enforcement authorities;
  - insurers; or
  - other relevant stakeholders.
23. Notification requirements will be determined based on the circumstances and applicable legal obligations.

## DELEGATION AND AUTHORISATION

24. Council authorises the Chief Executive Officer to:
- Implement this Policy,
  - appoint a Privacy Officer,
  - establish operational procedures and maintain the Information Breach Register.

# Information Breach Management

Shire of Donnybrook Balingup Council Policy EXE/CP-19



## LEGISLATION

- Privacy and Responsible Information Sharing Act 2024 (WA)
- Local Government Act 1995 (WA)
- Freedom of Information Act 1992 (WA)
- State Records Act 2000 (WA)
- Criminal Code Act Compilation Act 1913 (where applicable)

## APPENDIX

25. Nil.

## GOVERNANCE

### Related Policy(s):

- Records Management Policy (ADM/CP-1)
- Privacy and Responsible Information Sharing (EXE/CP-18)
- Cyber Security Policy (if applicable)
- Information Technology Acceptable Use Policy (if applicable)

### Related Procedure(s):

- Privacy Procedure.
- Information Breach Response Procedure (In progress)
- Privacy Impact Assessment Procedure (to be developed)
- Information Sharing Procedure (to be developed)

### Revision Requirements and Version Control:

|                                                |                                                           |                                       |                                                     |                                               |
|------------------------------------------------|-----------------------------------------------------------|---------------------------------------|-----------------------------------------------------|-----------------------------------------------|
| <b>Responsible Department(s):</b>              |                                                           | Executive                             |                                                     |                                               |
| <b>Review to be conducted by:</b>              |                                                           | Corporate Information Officer         |                                                     |                                               |
| <b>Revision Frequency:</b>                     |                                                           | <input type="checkbox"/> Annual (1yr) | <input checked="" type="checkbox"/> Triennial (3yr) | <input type="checkbox"/> Quinquennially (5yr) |
| <b>Current Version Date:</b>                   |                                                           | 23/09/2026                            | <b>Next Due:</b>                                    | 09/2029                                       |
| <b>Policy Version Details and Information:</b> |                                                           |                                       |                                                     |                                               |
| <b>#:</b>                                      | <b>Synopsis:</b>                                          | <b>Date:</b>                          | <b>Ref.:</b>                                        | <b>Record:</b>                                |
| 1                                              | Initial adoption of Information Breach Management Policy. | 23/09/2026                            | 171/09-26                                           | MONARCH-857934545-2001                        |