SHIRE OF NANNUP – Council Policy

Policy Number:	ADM29
Policy Type:	Administration
Policy Name:	Data Breach Policy
Policy Owner:	Chief Executive Officer
Date of Approval	
Council Resolution #	

POLICY STATEMENT

The Shire of Nannup (Shire) is committed to protecting personal information and complying with the *Privacy and Responsible Information Sharing Act 2024.*

Under the Privacy and Responsible Information Sharing Act 2024 (PRIS Act), public entities (including local governments) must have a Data Breach Policy to ensure timely identification, assessment, management and where a serious data breach is likely to cause harm, mandatory notification to the Information Commissioner and affected individuals in accordance with the Act.

Objective

To minimise damage caused by any data breaches by following the procedures aligned with the Data Breach Procedure.

Purpose

This Policy establishes the Shire's framework for preventing, detecting, assessing, reporting, and responding to data breaches involving personal information held by the Shire.

It is designed to prepare the Shire for compliance with the PRIS Act, including the Information Privacy Principles (IPPs) and the PRIS notifiable information breach scheme (commencing 1 January 2027) for serious breaches.

DEFINITIONS

Term	***Description***
Data Breach	A data breach occurs when personal information held by, or on behalf of the Shire (in electronic or hard copy form): • Is accessed without authority; • Is disclosed without authority; • Is lost in circumstances that are likely to result in unauthorised access or disclosure; or • Is accidentally or unlawfully destroyed, altered, or otherwise compromised.
Data Breach Response Plan	Detailed internal plan outlining the steps required for Shire staff to contain, access, investigate, and respond to an information breach.

Contracted Service Provider (CSP)	Private entity (or subcontractor) delivering services to a WA public entity under a state services contract. CSPs may be required to comply with PRIS via contractual clauses.
Eligible Information Breach	An eligible information breach occurs when **both** of the following conditions are met: 1. A data breach has occurred, involving personal information held by a public sector agency, including where the information: • is accessed without authority. • is disclosed without authority; or • is lost in circumstances where unauthorised access or unauthorised disclosure is likely to occur; and 2. A reasonable person would conclude that access, disclosure, or loss is likely to result in serious harm to an individual to whom the personal information relates.
Notifiable information breach (PRIS)	An assessed breach that meets PRIS criteria for notification to the WA Information Commissioner and affected individuals (commencing 1 Jan 2027).
Personal Information	Personal information means information or an opinion about an individual, whether: • true or not; and • recorded in any form or not; and • relating to a living or deceased individual, **where the individual is identifiable**, including where: • the individual's identity is apparent or can reasonably be ascertained from the information or opinion; or • the individual can be identified by reference to an identification number or other identifying particulars, such as a fingerprint, retinal scan, or body sample.

SCOPE:

This Policy applies to –

- The Shire of Nannup as a public entity under the PRIS Act (including Elected Members and employees when handling personal information in official duties).
- Contracted service providers (CSPs) that handle personal information for or on behalf of the Shire under a State services contract, where the contract stipulates PRIS compliance.
- All personal information in any form (electronic, paper, audio-visual) held or controlled by the Shire, including historical holdings (retrospectivity applies once PRIS privacy provisions commence).

Note: Under PRIS, local governments are "IPP entities." This Policy aligns with the 11 IPPs across the personal information lifecycle (collection, use, disclosure, storage, destruction) and embeds a notifiable information breach response consistent with PRIS definitions.

IMPLICATIONS:

This policy provides principles for the minimisation of any Data Breach.

The Shire will maintain and continually improve a Data Breach Management Program that:

1. Prevents breaches via appropriate controls, training, and security practices (aligning to IPPs and best practice).

2. Detects and responds to suspected breaches promptly, following a structured 4-step incident process compatible with OAIC guidance (Contain → Assess → Notify → Review).

3. Assesses "serious harm" using PRIS/OAIC criteria and documents decisions in an Incident Assessment Report.

4. Reports and notifies PRIS notifiable information breaches to the WA Information Commissioner and affected individuals from 1 January 2027, in accordance with PRIS timelines and format requirements, and as soon as practicable after assessment.

5. Where Commonwealth OAIC obligations apply (e.g., Shire acts as an APP entity for certain federal programs), the Shire will mirror OAIC NDB requirements, ensuring integration with PRIS where both apply.

6. Manages contractors (CSPs) so contracts expressly require PRIS-compliant breach notification flows and cooperation with the Shire's response procedures.

7. Records all breaches (suspected and confirmed) in a secure register and reports systemic issues to the Executive and where required to the Audit, Risk and Improvement Committee as part of continuous improvement.

8. Engages with affected individuals respectfully, transparently, and in culturally appropriate ways, including consideration of Aboriginal data governance principles in PRIS.

IMPLEMENTATION:

Data Breach Response (Summary)

The Shire will implement a detailed Information Breach Response Procedure (refer separate document) that follows best practice and aligns with PRIS and OAIC:

Step 1 — Contain & Secure

- Isolate systems, revoke compromised credentials, preserve evidence/logs, and engage ICT/third-party vendors as required.

- Begin a preliminary risk assessment (nature of data, sensitivity, volume, exposure).

Step 2 — Assess & Decide (Serious Harm Test)

- Conduct a documented assessment to determine if the breach is notifiable under PRIS (from 1 Jan 2027).
- Use the “serious harm” test (likelihood) with the PRIS/OAIC factors; consult legal/forensic expertise if needed.

Step 3 — Notify (If Notifiable)

- Prepare formal notifications for the WA Information Commissioner and affected individuals (content includes description, types of information, protective steps, and remedial actions).
- Provide clear support options (hotline/email) and protective advice (e.g., password resets, credit watch).
- Coordinate communications with WA Information Commissioner’s Office and, if relevant, OAIC (where federal programs apply).

Step 4 — Review & Improve

- Identify root causes and implement corrective actions (policy, technical controls, training).
- Update the breach register and include metrics in quarterly Executive/Audit, Risk and Improvement Committee reports.

Timelines and thresholds

- PRIS notifiable scheme requires notification where serious harm is likely; the Shire will operate on a “as soon as practicable” basis after completing assessment, mirroring OAIC practice.

Contract Management (CSPs)

- All relevant State services contracts must include a data breach clause requiring CSPs to immediately notify the Shire of any suspected or confirmed breach, to cooperate with assessments, and where applicable, to assist with PRIS and OAIC notifications.
- CSPs must maintain a Data Breach Response Plan compatible with this Policy.

Training & Awareness

- The Shire will run mandatory privacy and breach-response training for staff and contractors, with refreshers following major breaches or technology changes.
- Executives and Coordinators will receive tailored training on serious harm assessments, PRIS notification duties, and media/communications management.

Security Controls & Preventative Measures

- Maintain a risk-based cyber security posture, physical security, and robust access controls and audit trails.

AUTHORITIES AND ACCOUNTABILITIES:

There is no requirement for the CEO to delegate or authorise a decision-making function to an employee for efficiency regarding this policy.

ROLES AND RESPONSIBILITIES

1. Council: Approves this Policy and receives significant risk updates through the Audit, Risk and Improvement Committee.

2. CEO (Principal Officer): Accountable for ensuring PRIS compliance, adequate resourcing, and endorsing serious breach notifications and communications.

3. All Executive Managers are responsible for the implementation of the policy within their respective units.

4. Privacy and Responsible Information Sharing Officer:

    a) Maintains the Data Breach Response Procedure, breach register, training and audit.
    b) Coordinates assessments, drafts notifications and liaises with the Information Commissioner and the public.
    c) Is responsible for the publication of and compliance with this policy and supporting procedures and providing interpretations in the event of the need for clarification.

5. ICT: Leads technical containment, forensic logs, evidence preservation, and vendor engagement; ensures cyber-security measures are maintained and improved.

6. Managers/Coordinators: Ensure their areas and CSP contracts incorporate PRIS obligations (including the breach clause) and escalate breaches immediately per Procedure.

7. All Staff and Contractors: Must report suspected breaches immediately via the nominated channels and follow training and directions.

DISPUTE RESOLUTION

All disputes regarding this policy will be referred to by the Executive Manager Corporate Services in the first instance. In the event an agreement cannot be reached, the matter will be submitted to the CEO for a ruling.

EVALUATION AND REVIEW

The impact of the policy will be evaluated by:

Review of complaints of unauthorised collection, storage or sharing of Personal Information.

The policy is to be reviewed every three (3) years from its approval date, or more frequently if appropriate in line with legislative changes.

RELATED DOCUMENTS

Shire of Nannup Complaints Policy
Privacy Information Sharing Policy (PRIS) Act 2024.

REFERENCES

Privacy and Responsible Information Sharing Act 2024

RESPONSIBILITY FOR IMPLEMENTATION

Privacy and Responsible Information Sharing Officer

Version OCM Ref. #	Date:	Next Review	ECM Reference #
1.			
2.			
3.			