



1/034 Information Management Policy

Objective

The objective of this policy is to state the Town of Port Hedland's (the Town) commitment to manage the Town's information. Information, its integrity and security, is critical to how the Town makes decisions, acts transparently, demonstrates accountability, collaborates, develops policy and delivers services to the Town and broader community. This commitment will achieve compliance with all applicable State Legislation, Regulations and Standards.

Content

Scope

This policy applies to the Elected Members, staff and contractors of the Town of Port Hedland and all information assets (records, information and data) in any format, created or received to support the Town's business activities.

It covers all business applications used to create, manage and store information assets, including dedicated information management systems, business systems, databases, email, voice and instant messaging, websites and social media applications.

This policy covers information created and managed in-house and off-site including in cloud-based systems.

Principles

Information is critical to the Town, government and the Port Hedland community.

The Town will operate under these information principles:

Principle 1: Information is valued and governed as an asset.

Information is essential to Town operations and will be reliably maintained as authentic evidence of business activity to ensure value in decision making and delivery of services.

Principle 2: Information is created and managed digitally.

Digital information and end to end digital processes will be the default position, with hardcopy records managed by exception. Systems support good information management as part of business processes. Integration of systems must support easy creation and capture of records of business activity.

Principle 3: Information is fit for its intended purposes and is easy to find, access and use.

Information must be accurate, authentic and trusted, to allow ongoing use and reuse by the Town and the community. Information will be created and managed based on its operational and strategic importance, its risk profile, and the needs of all its users. It must be kept and remain accessible to authorised users for as long as required.



Principle 4: Information management is embedded into Town business activities.
The Town will build information management into all business systems and all aspects of training including sharing, release, discovery, data quality, de-identification and security of information.

Principle 5: Information is protected from unauthorised use and loss.
Information will be managed from receipt or creation to protect personal and sensitive information and prevent deletion until official authorisation. It must be disposed of in a systematic and auditable way.

Definitions

“Business Activities” major tasks performed by the Town as part of its responsibilities for achieving the strategic goals of the Town on behalf of the Community.

“Business System” an automated system that creates or manages data about an organisation’s activities, including applications whose primary purpose is to facilitate transactions between an organisational unit and its customers.

“Confidentiality” property that information is not made available or disclosed to unauthorised individuals, entities or processes.

“Database” is an electronically stored, systematic collection of data. It includes words, numbers, images, videos, and documents in various ways.

“Information” is knowledge communicated or received. It is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

“Information Assets” an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions, thereby satisfying a recognised agency requirement.

“Information Security” is preservation of confidentiality, integrity and availability of information.

“Integrity” property of accuracy and completeness.



Relevant legislation	<ul style="list-style-type: none">▪ State Records Act 2000.▪ Local Government Act 1995▪ Freedom of Information Act 1992▪ Evidence Act 1906
Relevant Standards	<ul style="list-style-type: none">▪ AS/ISO 15489 Records management▪ ISO 27000 Information Security Management Systems▪ SA/SNZ TR 18128 Risk Assessment for records processes and systems▪ State Records Office of Western Australia State Records Commission Standards
Delegated authority	Senior Records Officer
Business unit	Digital Services
Directorate	Corporate Services
Supporting Documents	<ul style="list-style-type: none">▪ Information Management Procedures▪ Digital Roadmap 2024 to 2027
Related Documents	<ul style="list-style-type: none">▪ Information Classification Policy▪ Risk Management Policy▪ Data Breach Policy



<i>Governance to complete this section</i>			
Version Control	Version No.	Resolution No.	Adoption date
	V01	CM202425/192	27 November 2024
Review frequency	Annually		

Document Control Statement – The electronic reference copy of this Policy is maintained by the Governance Team. Any printed copy may not be up to date and you are advised to check the electronic copy at <http://www.porthedland.wa.gov.au/documents/public-documents/policies> to ensure that you have the current version. Alternatively, you may contact the Governance Team.