Information Management Policy

Public Records Act 2002

1. Policy Statement

The Townsville City Council (Council) values information as a core strategic asset.

This policy establishes the information principles to enable consistent management of information throughout its lifecycle, from creation to final disposal. Council will manage information in accordance with all information management governance artefacts, including the Records Governance Policy, Records Governance Administrative Directive and Information Management Administrative Directive and Records and Information Management Procedure.

2. Principles

Information management is the practice of collecting, organising, securing, storing, retrieving, disseminating, and disposing of information in compliance with legislation. It involves the management of digital and physical information to facilitate effective decision-making, improve operational efficiency, and support various business processes.

Council holds information about a range of matters relating to Council business. Information management is of key importance to good governance and is achieved through Council's Information Management Framework, which sets out the hierarchy of business artefacts including Policies, Administrative Directives, Procedures and required tools.

3. Scope

This Information Management Policy, in conjunction with the Records Governance Policy, applies to all Information Assets held by the Council and must be followed by Councillors and Workers.

Further, this policy acknowledges the Information Management Framework, which contributes to effective management of information across Council, including:

- Information Governance;
- Knowledge Management;
- Information Asset Management;
- Information Access and Use Management;
- Recordkeeping;
- Data Management; and,
- Information Security.

Document No. 24397167
Authorised by – Chief Executive Officer
Document Maintained by – Information Technology Services

Version No.4
Initial Date of Adoption (Version 1) – 22.02.11
Current Version Reviewed – 19.06.24
Next Review Date – 19.06.28

Information Technology Services | **Information Management Policy**

PAGE 1 OF 4

4.   Responsibility

The Chief Executive Officer is responsible for ensuring that this policy is understood and adhered to by all Councillors and Workers.

Councillors and Workers are responsible for ensuring their own adherence to this policy.

5.   Definitions

Decision Rights Model – provides leadership, advice, and direction on records and information management for the whole of Council.

Information Asset – means:

- 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; or
- A piece of information stored in any manner, which is recognised as 'valuable to the organisation'.

  It is usually subject to a lifecycle (create, access, distribute, store, and dispose) that is defined either explicitly within policy or procedure or implicitly within a business system.

Information Asset Management – means a focus on full lifecycle management of information as an asset and classifying it so it can be found and used.

Information Management Framework – identifies and defines governing documents which contribute to effective information management and serves as an organising framework for ensuring policy coverage.

Information Security – means a focus on confidentiality, integrity and availability of information guided by the ISO 27001 Information Security Management Systems international standard.

Integrity of Information – is the dependability or trustworthiness of information. More specifically, it is the accuracy, consistency and reliability of the information content, process and system.

Knowledge Management – means the formal process of identifying, organising, storing and sharing of information assets including the approach/methods for managing uncaptured knowledge of Workers within Council.

Sensitive Data – information containing personal information, legal or law enforcement operations or commercial interest that could significantly affect the competitive process and provide an unfair advantage.

Suite of Programs - An automated system designed to manage semi-structured or unstructured content including text, images and video content. A subset of the documents managed in an electronic Documents and Records Management Solution (eDRMS) can be declared to be records. The current eDRMS is the Enterprise Content Manager, hosted in CIAnywhere, manages these records and preserves the record's context, authenticity and integrity.

Workers – includes employees, contractors, volunteers, and all others who perform work on behalf of council.

Document No. 24397167
Authorised by – Chief Executive Officer
Document Maintained by – Information Technology Services

Version No.4
Initial Date of Adoption (Version 1) – 22.02.11
Current Version Reviewed – 19.06.24
Next Review Date – 19.06.28

Information Technology Services | **Information Management Policy**

PAGE 2 OF 4

6. Policy

Council values its information which must be proactively managed through sharing, access and maintenance with appropriate security and governance.

This policy provides a basis for Administrative Directives, Procedures and tools to assist in establishing business unit requirements in specific areas.

6.1. Information Is an Asset

Treating information as an asset means recognising its value, investing in its management, protecting it from risks, and leveraging it to achieve organisational goals. This approach acknowledges that information is a critical resource that, when managed effectively, can significantly contribute to an organisation's success.

6.2. Information Is Readily Available and Can Be Accessed by Those Authorised to Receive It

Council recognises the importance of enabling authorised users to easily find and access relevant information. Council achieves this by:

- organising information logically;
- implementing efficient search tools; and,
- providing user-friendly interfaces.

Workers enable swift access to information through the consistent application of metadata, categorisations and security classifications.

This approach promotes effective decision-making, collaboration and productivity. Additionally, Council encourages and advocates for adoption of technology and user-friendly strategies to enhance navigation within its information repositories.

6.3. Information Is Compliant throughout Its Lifecycle

This principle maintains Council's commitment to managing information in accordance with legislation from creation to disposal. This involves maintaining accuracy and security at all stages, including collection, storage, usage, sharing and disposal of the information. This principle helps Council mitigate information risks, protect sensitive data and maintain trust with stakeholders (internally and externally).

6.4. Information Is Secure and Confidential where Required

This principle underscores the importance of safeguarding Sensitive Data through suitable measures such as implementing security controls and auditing procedures. Through the implementation of controls, Council can protect confidential information, adhere to information privacy principles and foster trust with stakeholders.

6.5. Information Is Monitored to Maintain Integrity and Ensure Quality

Integrity of information must be maintained by relevant custodians to enable quality of information. Integrity will be reduced where inappropriate or unauthorised changes of information occur. The

Document No. 24397167
Authorised by – Chief Executive Officer
Document Maintained by – Information Technology Services

Version No.4
Initial Date of Adoption (Version 1) – 22.02.11
Current Version Reviewed – 19.06.24
Next Review Date – 19.06.28

Information Technology Services | **Information Management Policy**

PAGE 3 OF 4

higher the integrity requirement, the more control should be implemented to safeguard information against inappropriate or unauthorised change.

Quality of information will be assured by consistently overseeing data to assess accuracy relevance and reliability.

By implementing monitoring processes, Council can identify and rectify errors, inappropriate or unauthorised changes, inconsistencies and outdated information to maintain data quality and integrity over time.

7. Legal Parameters

Information Privacy Act 2009

Local Government Act 2009

Local Government Regulation Act 2012

Public Records Act 2002

Public Sector Ethics Act 1994

Right to Information Act 2009

8. Associated Documents

Complaints Management Policy

Confidentiality Policy

General Retention and Disposal Schedule

General Retention and Disposal Schedule for Digital Source Records: QDAN 678 v.1

Information Privacy Policy

Local Government Sector Retention and Disposal Schedule

Right to Information Policy

Records Governance Policy

Water Retention and Disposal Schedule QDAN 738 v1

Document No. 24397167
Authorised by – Chief Executive Officer
Document Maintained by – Information Technology Services

Version No.4
Initial Date of Adoption (Version 1) – 22.02.11
Current Version Reviewed – 19.06.24
Next Review Date – 19.06.28

Information Technology Services | **Information Management Policy**

PAGE 4 OF 4