

From: [LGOIMA](#)
To: [REDACTED]
Subject: RE: LGOIMA request - Information Management Policies and Frameworks - Reference: 2474
Date: Wednesday, 6 November 2024 12:52:57 pm
Attachments: [IS23 Policy on Generative Artificial Intelligence.pdf](#)
[IM01 Information Management Policy.pdf](#)
[IM02 Information Ownership Policy.pdf](#)
[IM03 Information in Content and Format Policy.pdf](#)
[IM04 Information Security and Access Policy.pdf](#)
[IM05 Information Lifecycle Management Policy.pdf](#)

Kia ora [REDACTED],

We refer to your official information request dated 30 October 2024. Our response is below:

- **Information (or Records) Management Policy**

Please find attached records/information management policies held by Council.

- *"IM01 Information Management Policy.pdf"*
- *"IM02 Information Ownership Policy.pdf"*
- *"IM03 Information in Content and Format Policy.pdf"*
- *"IM04 Information Security and Access Policy.pdf"*
- *"IM05 Information Lifecycle Management Policy.pdf"*

- **Digital Preservation Strategy**

- **Digital Business Strategy**

With regards to the digital preservation and digital business strategy. We have our Digital Strategy that we call our "Blueprint for Tasman's Digital Future" that is publicly available for viewing on our website via the following link - [Blueprint for Tasman's Digital Future | Tasman District Council](#)

- **AI Policy**

Please find attached the AI policy held by Council:
- *"IS23 Policy on Generative Artificial Intelligence.pdf"*

If you are unsatisfied with the Council's response, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Yours sincerely,
Legal Services Officer

IS23 Policy on Generative Artificial Intelligence use

INFORMATION SERVICES POLICY

POLICY REFERENCES	
Sponsor:	Information Services Manager
Internal review due:	Jan 2024
Legal compliance:	<ul style="list-style-type: none"> • IS06 – Appropriate use of Internet and Online Services • HR13 Code of Conduct • Privacy Act 2020 • Harmful Digital Communications Act (HDCA) 2015 • Local Government Official Information and Meetings Act 1987
Associated Documents/References	
Policy Number	IS23
Approved by Chief Executive	FINAL
Approved by Council (If applicable)	N/A

Policy Contents

Purpose

Application

Background

Scope

Policy Statement

Principles

Purpose

The purpose of this policy is to confirm the objectives and responsibilities of the use of Generative Artificial Intelligence (Generative AI) within council.

It forms a statement of high-level commitment to the principles, relevant to Generative AI, by which the organisation will operate.

Application

This policy applies to all Council staff who utilise Generative AI for work purposes or who use Generative AI for personal use on Council devices.

Background

Generative AI, like Chat-GPT, refers to artificial intelligence systems that can create original and creative content, such as images, text, music, or videos, by learning patterns and structures from large datasets. It involves the use of deep learning techniques and has applications in various fields, including art, design, and data augmentation. However, ethical considerations are important due to the potential misuse of Generative AI for fabricating realistic but false content.

Council staff need to be especially careful of how they use these tools to meet their obligations to both the Council under the code of conduct and their wider Privacy Act obligations.

Scope

This policy applies to Council's use of Generative AI across the council and include all data and information contained within systems.

The rapidly developing landscape for Generative AI solutions, use and outputs is such that this policy should be reviewed every six months through to the end of 2024 with a further determination of the review frequency to be considered at that time.

Policy Statement

The Council will manage the use of Generative AI in a safe, legally compliant, co-ordinated manner to ensure the safety and privacy of staff and citizens is maintained.

Principles

The Council will adhere to the following principles in its use of Generative AI:

Compliance with Laws and Ethical Standards:

Emphasise the requirement to comply with all applicable laws, regulations, and ethical guidelines when using Generative AI. Highlight the importance of respecting privacy, confidentiality, intellectual property rights, and avoiding any harmful or illegal activities.

Responsible Use:

Encourage responsible use of Generative AI by promoting transparency, fairness, and accountability. Users should be aware of the potential impact of generated content and should strive to minimise risks associated with misinformation, manipulation, or bias.

Maintain Privacy and Data Protection:

It is important that the use of Generative AI protects personal information and data privacy. Generative AI usage must comply with the Privacy Act 2020 and staff member obligations with respect to maintaining confidentiality.

Avoid Harmful or Offensive Content:

Prohibit the generation of content that is harmful, abusive, offensive, or discriminatory. Users must not create or distribute content that incites violence, promotes hatred, or violates the dignity of individuals or groups.

Transparency and Disclosure:

Users must clearly disclose when generated content is not created by a human, indicating its origin and nature. Transparently distinguishing between human-generated and AI-generated content helps prevent confusion or deception.

Regular Review and Updates:

Emphasise the need to periodically review and update the acceptable use policy to address emerging challenges, advances in technology, or changes in legal or ethical standards.

Use of Generative AI

Staff should be able to use Generative AI for Council business if;

- There is a valid business reason for using it.
- They do not, for security reasons, use their Council credentials to register with a Generative AI service, solution or tool.
- Council information that is not in the public domain or intended for the public domain is not uploaded or otherwise made available to any Generative AI service, solution or tool.
- There is no possibility that personal Information relating to any person is uploaded or otherwise made available to any Generative AI service, solution or tool.
- All Information generated by Generative AI tools is reviewed and scrutinised for accuracy and bias and that such review is noted.
- Artifacts produced using generative AI are acknowledged as such within, or on, the artifact itself.
- Copyrighted material used to create the output is acknowledged together with the right to use such material

Receiving content from Generative AI

If staff use material that was created using generative AI, they must acknowledge it before using it in reports, workshop materials, or other council activities.

Conduct and behaviour when using Generative AI

Staff are expected to uphold the same high standards of conduct and behaviour online as they would in any other workplace setting, as outlined in:

- Policy HR13 Code of Conduct.
- Privacy Act 2020.

This includes:

- Remaining politically neutral, impartial, and professional.
- Interacting with respect, courtesy, and without engaging in harassment or intentionally incendiary comments.
- Handling information appropriately, recognising the need for confidentiality in certain cases.
- Taking all reasonable steps to ensure that there is no link to materials that are defamatory, harassing, indecent, objectionable, or contrary to official government advice and guidelines, as outlined in policy IS06 – Appropriate Use of Internet and Online Services.
- Adhering to the Harmful Digital Communications Act 2015.
- Taking reasonable steps to avoid conflicts of interest.
- Staff must fully comprehend Tasman District Council's values, the expected Code of Conduct, and their application to official and personal communications.

Failure to comply with the Generative AI Policy may result in disciplinary action in accordance with the Council's Code of Conduct.



Authorised by:

Janine Dowding, Chief Executive

Following LT approval on 17 July 2023

Information Management Policy

ORGANISATIONAL POLICY

POLICY REFERENCES

Sponsor:	Group Manager- Information, Science and Technology.
Effective date:	
Internal review due:	June 2024
Legal compliance:	Public Records Act 2005 Local Government Official Information & Meetings Act 1987 Privacy Act 2020 Contract & Commercial Law Act 2017 Information and Records Management Standard 2016
Associated Documents/References:	IM 02 Information Ownership Policy IM 03 Information Context Policy IM 04 Information Security and Access Policy IM 05 Information Lifecycle Management Policy IS 03 IS Documents and File Locations
Policy Number:	IM 01

Contents

1.....	Purpose	2		
2.....	Definitions	2		
3.....	Application	3		
4.....	Policy	3		
4.1.Supporting	Policies	3		
4.2.Supporting	Documents	4		
4.3.Why	Manage	Information?	4	
4.4.Mandatory	Requirements	4		
4.5.Compliance	with	IM	Policies	5
5.....	Approval	5		

1. Purpose

The Tasman District Council (the Council) is committed to establishing and maintaining Information Management practice that meet its business and statutory requirements and maintains practical effective and efficient processes that support customer expectations.

The purpose of the set of Information Management policies is to provide the necessary foundation for improvement in the Council's information and records management practice, which will, in turn, ensure that the Council meets its obligations to manage the information and records it creates and receives in the course of conducting business.

Specific procedures for managing both digital and hard-copy information are documented in the Council's Information Management Procedures.

2. Definitions

EDRMS - Electronic Document and Record Management System, a database which contains and manages files. All changes and versions are controlled. Benefits include reduced risk of data loss, document searchability, and opportunities to create more structured and information-rich documents.

IM- Information management

3. Application

This policy applies to:

- All employees
- All elected members
- All contractors, consultants and authorised third parties (including Directors of Council Controlled organisations and appointees to subcommittees).
- All aspects of the Council's operations, in whatever manner it is conducted and in whichever location it is carried out
- All business applications and processes used to create information and records.
- All information regardless of media or format which is generated or received as part of Council business.
- All information held in all operating environments, including information held in service arrangements.

4. Policy

1. Tasman District Council's information and records are recognised as a key strategic and highly valuable asset.
2. Tasman District Council's information management framework will be aligned with the requirements of the Public Records Act 2005.
3. Tasman District Council will create and maintain records to support good business practice.
4. Tasman District Council will apply retention periods and appropriate disposal actions to all Council information.
5. Council information must be managed in approved EDRMS.
6. The Council's paper records must be managed in line with the requirements set out by Archives New Zealand.

4.1. Supporting Policies

This policy statement is supported by specific policy relating to aspects of information management:

- IM 02 Information Ownership Policy
- IM 03 Information Content and Format Policy
- IM 04 Information Security and Access Policy
- IM 05 Information Lifecycle Management Policy

4.2. Supporting Documents

This suite of policies is supported by the following documents and resources:

- IM Procedures
- IM Definitions (a glossary of key IM terms)
- IM Repositories (a list of approved Council information repositories and systems)
- IM Roles and responsibilities
- IM Legislative environment
- IM Value of information guide
- IM Lifecycle diagram

4.3. Why Manage Information?

Good IM practice allows Council to manage risk by recording business decisions and processes, increasing transparency and allowing Council to make informed decisions. Managing information and records is important because it:

- Enables the public to hold the government accountable
- Provides the foundation for sustainable and effective products and services
- Supports decision making
- Outlines responsibilities
- Documents rights and entitlements
- Drives collaboration and communication
- Facilitates and enables creativity and growth
- Preserves public knowledge for discovery and reuse
- Makes up the corporate memory of an organisation.

4.4. Mandatory Requirements

Some information about the Council's operations is regulated by statutory and regulatory requirements. Good IM practice ensure that Council creates, captures, retains and maintains evidence of compliance with these requirements. The key legislation in New Zealand concerning IM in the local authority sector that impacts on Council is as follows:

- Contract and Commercial Law Act 2017
- Local Government Official Information and Meetings Act 1987
- Privacy Act 2020
- Public Records Act 2005

It is important to note that there is other legislation specific to Council operations that contains requirements for the management of information relating to specific functions of activities of Council, such as the Resource Management Act 1991 and the Building Act 2004.

In addition, Council is required to adhere to the mandatory Information and Records Management Standard 2016 released by the Chief Archivist.

4.5. Compliance with IM Policies

Failure to comply with Information Management policies could result in disciplinary action as detailed in the Council's HR13 Code of Conduct.

5. Approval

Current version approver name and position

Authorised by

Steve Manners

Group Manager – Information Science and Technology



Date of approval: 08/09/2022

Date Version Approved	Change Details	Officer sign-off
19/11/19	Initial Policy Approval	Chief Executive
08/08/2022	Minor changes	Group Manager- Information, Science and Technology.

Information Ownership Policy

ORGANISATIONAL POLICY

POLICY REFERENCES

Sponsor:	Group Manager- Information, Science and Technology.
Effective date:	
Internal review due:	June 2024
Legal compliance:	Public Records Act 2005 Information and Records Management Standard 2016
Associated Documents/References:	IM 01 Information Management Policy
Policy Number:	IM 02

Contents

1.....	Purpose	2
2.....	Definitions	2
3.....	Application	3
4.....	Policy	3
4.1.Ownership and Custodianship of Information		3
4.2.Public Information		3
4.3.Council Departments are Custodians for Information Core to their Functions and Activities		3
4.4.Individual Employee Responsibilities		4
4.5.Compliance with IM Policies		4
5.....	Approval	4

1. Purpose

The purpose of the Information Ownership Policy is to inform Council staff about their requirements in specific aspects of Information Management, and to enable them to make informed decisions on the information they are managing. This policy sets out the ownership standard of information and records created or received by those covered by the application of this policy in the course of their work for the Council.

2. Definitions

BAU- Business as usual

EDRMS- Electronic Document and Record Management System, a database which contains and manages files. All changes and versions are controlled. Benefits include reduced risk of

data loss, document searchability, and opportunities to create more structured and information-rich documents.

3. Application

This policy applies to:

- All employees
- All elected members
- All contractors, consultants and authorised third parties (including Directors of Council Controlled organisations and appointees to subcommittees).
- All aspects of the Council's operations, in whatever manner it is conducted and in whichever location it is carried out
- All business applications and processes used to create information and records.
- All information regardless of media or format which is generated or received as part of Council business. It applies to all information held in all operating environments, including information held in service arrangements.

4. Policy

4.1. Ownership and Custodianship of Information

All information and records created or received by those covered by the application of this policy in the course of their work for the Council is owned by the Council. Council protects and provides access to that information in its role as guardian and custodian and is responsible for its appropriate management throughout its lifecycle.

The Chief Executive Officer and Leadership Team have overall responsibility and accountability for the information owned by Council. The Executive Sponsor for Information Management is Council's representative both to the organisation and to Archives New Zealand's regulatory framework.

4.2. Public Information

All information created or received by those covered by the application of this policy in the course of their work for the Council is public information and are considered Local Authority Records under the Public Records Act. Local Authority Records should be classified as Open Access as prescribed by the Public Records Act, unless there are agreed acceptable grounds for withholding access such as other legislative requirements (e.g. Privacy Act/Local Government Official Information and Meetings Act 1987).

4.3. Council Departments are Custodians for Information Core to their Functions and Activities

Each business unit in Council is custodian for the information that is core to their functions and activities. This includes requirements to create, maintain, and manage all information in line with Council Information Management procedures.

Information Management requirements must be considered in all projects, contracts and other procedures of business.

4.4. Individual Employee Responsibilities

All those covered by the application of this policy are responsible for managing any Council information in line with the responsibilities outlined in Policy IM 1.0 and Council Information Management Procedures. All those covered by the application of this policy must approach their responsibilities to Information Management with the mindset that they are in public service roles, acting as custodians of the information they use in the conduct of their work.

It is the responsibility of all those covered by the application of this policy to have documents and emails pertaining to the business of the Council filed within the correct EDRMS. This must be a part of BAU practices, and prior to departure from Council all public records must be filed correctly. This responsibility falls on the individual.

4.5. Compliance with IM Policies

Failure to comply with Information Management policies could result in disciplinary action as detailed in the Council's HR13 Code of Conduct.

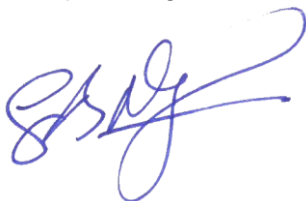
5. Approval

Current version approver name and position

Authorised by

Steve Manners

Group Manager – Information Science and Technology



Date of approval:

08/09/2022

Date Version Approved	Change Details	Officer sign-off
19/11/19	Initial Policy Approval	Chief Executive
DD/MM/YY	Minor changes	Group Manager- Information, Science and Technology.

--	--	--

Information in Content and Format Policy

ORGANISATIONAL POLICY

POLICY REFERENCES

Sponsor:	Group Manager- Information, Science and Technology.
Effective date:	
Internal review due:	June 2024
Legal compliance:	Public Records Act 2005 Information and Records Management Standard 2016
Associated Documents/References:	IM 01 Information Management Policy IS 03 IS Documents and File Locations
Policy Number:	IM 03

Contents

1.....	Purpose	2
2.....	Definitions	2
3.....	Application	2
4.....	Policy	3
4.1.Content and Context Define Information		3
4.2.....	Format	3
4.3.....	Metadata	3
4.4.Compliance with IM Policies		3
5.....	Approval	3

1. Purpose

The purpose of the Information in Content and Format policy is to inform Council staff about their requirements in specific aspects of Information Management, and to enable them to make informed decisions on the information they are managing. Specifically with regard to managing information based on the content of a record, rather than the format that it is presented in.

2. Definitions

Metadata – Metadata is data that provides context, content and structure of records and their management over time. It also allows data to be sorted, ordered, and retrieved. It is data about data.

3. Application

This policy applies to:

- All employees
- All elected members
- All contractors, consultants and authorised third parties (including Directors of Council Controlled organisations and appointees to subcommittees).

- All aspects of the Council's operations, in whatever manner it is conducted and in whichever location it is carried out
- All business applications and processes used to create information and records.
- All information regardless of media or format which is generated or received as part of Council business. It applies to all information held in all operating environments, including information held in service arrangements.

4. Policy

4.1. Content and Context Define Information

The Council recognises that its information assets exist in the information content and context **not** the format or media the information is presented in, i.e. information will be managed by the context of the content rather than the format presented. For example, customer interaction may be via email, hard copy letter, by phone or in person. It is the subject of interaction that is important to record and manage, not the way it is received.

4.2. Format

The **primary** format for information within Council moving forward is **digital**. This means that all those covered by the application of this policy are expected to manage digital information of all activities within Council's business systems and official Council repositories. This includes both born-digital and digitised information.

Where digitisation of information is required, Council will provide appropriate resources to enable the transfer to digital. This will often require review and development of the related business process. [Any digitisation must conform to a minimum set of specifications and standards that support our ongoing organisational requirements. Guidance and assistance with digitisation of documents and records can be received from the Information Management team.](#)

Where continued management of hardcopy information is appropriate, the same policies and procedures for the management of information are applicable.

4.3. Metadata

When creating or receiving information, all those covered by the application of this policy will capture all relevant contextual and technical metadata to ensure that information is meaningful, findable, and reusable.

4.4. Compliance with IM Policies

Failure to comply with Information Management policies could result in disciplinary action as detailed in the Council's HR13 Code of Conduct.

5. Approval

Current version approver name and position

Authorised by

Steve Manners

Group Manager – Information Science and Technology



Date of approval:

08/09/2022

Date Version Approved	Change Details	Officer sign-off
19/11/19	Initial Policy Approval	Chief Executive
08/09/2022	Minor changes	Group Manager- Information, Science and Technology.

Information Security and Access Policy

ORGANISATIONAL POLICY

POLICY REFERENCES	
• Sponsor:	Corporate Services Manager
• Effective date:	25 September 2019
• Internal review due:	25 September 2020
• Legal compliance:	Public Records Act 2005 Information and Records Management Standard 2016
• Associated Documents/References	IM 01 Information Management Policy LGOIMA Request Policy IS 03 IS Documents and File Locations 2014 IS 05 Email Use by Employees and Elected Officials IS 07 Cybersecurity 2018
• Policy Number	IM 04
• Approved by Chief Executive	Yes
• Approved by Council (If Applicable)	N/A

Policy Contents

[Purpose](#)

[Application](#)

[Information Security](#)

[Access](#)

[Unauthorised Distribution of Information](#)

[Compliance with IM Policies](#)

Purpose

The purpose of Information Management supporting policy statements is to inform Council staff about their requirements in specific aspects of Information Management, and to enable them to make informed decisions on the information they are managing.

Application

This policy applies to:

- All employees
- All elected members
- All contractors, consultants and authorised third parties (including Directors of Council Controlled organisations and appointees to subcommittees).
- All aspects of the Council's operations, in whatever manner it is conducted and in whichever location it is carried out
- All business applications and processes used to create information and records.

- All information regardless of media or format which is generated or received as part of Council business. It applies to all information held in all operating environments, including information held in service arrangements.

Information security

All those covered by the application of this policy **must** use Council's business systems and IM processes to ensure that all private and sensitive information is appropriately classified and protected against unauthorised access. The security of information will be considered before access is provided.

Access

Information **will** normally be available and classified as Open Access to all those covered by the application of this policy unless there is a specific reason to preclude access (i.e. considerations of privacy, legal professional privilege, commercial sensitivity, statutory requirements etc.).

All those covered by the application of this policy will be held **accountable** for accessing information inappropriately (i.e. without a valid business reason).

Access to information by members of the public and external organisations is governed by specific legislation (namely the Local Government Information and Meetings Act 1987 and the Privacy Act 1993) and may be subject to other legal considerations. Reasons for refusing access to requested information can be found in the [LGOIMA Request Policy](#).

Confidential Information

Information deemed to be confidential, including but not restricted to

- Confidential meeting minutes
- Contract information containing commercial sensitivity
- Sensitive Employee or other information deemed protected under the Privacy Act 1993

Where information is deemed confidential, access will be limited to only those parties with an acknowledged authority to it.

Unauthorised Distribution of Information

Council information, though primarily public information, should only be distributed to authorised recipients, both internal and external.

All those covered by the application of this policy will be held **accountable** for distributing information to unauthorised recipients (i.e. without a valid business reason and appropriate authorisation).

Compliance with IM Policies

Failure to comply with Information Management policies could result in disciplinary action as detailed in the Council's HR13 Code of Conduct.



Authorised by

19.11.19

Date of approval:

Information Life Cycle Management Policy

ORGANISATIONAL POLICY

POLICY REFERENCES

Sponsor:	Group Manager- Information, Science and Technology.
Effective date:	
Internal review due:	June 2024
Legal compliance:	Public Records Act 2005 Information and Records Management Standard 2016
Associated Documents/References:	IM 01 Information Management Policy IS 03 IS Documents and File Locations IS 05 Email Use by Employees and Elected Officials
Policy Number:	IM 05

Contents

1.....	Purpose	2
2.....	Definitions	2
3.....	Application	2
4.....	Policy	3
4.1.Creation	and receipt of information	3
4.2.Use	of information	3
4.3.Using	official repositories	3
4.4.Information	Disposal	3
4.5.Compliance	with IM Policies	4
5.....	Approval	4

1. Purpose

The purpose of the Information Life Cycle Management policy is to inform Council staff about their requirements in specific aspects of Information Management, and to enable them to make informed decisions on the information they are managing. Specifically with regard to the life cycle of information created or received in the course of daily business by those covered by the application of this policy.

2. Definitions

IM- Information Management

3. Application

This policy applies to:

- All employees

- All elected members
- All contractors, consultants and authorised third parties (including Directors of Council Controlled organisations and appointees to subcommittees).
- All aspects of the Council's operations, in whatever manner it is conducted and in whichever location it is carried out
- All business applications and processes used to create information and records.
- All information regardless of media or format which is generated or received as part of Council business. It applies to all information held in all operating environments, including information held in service arrangements.

4. Policy

4.1. Creation and receipt of information

All those covered by the application of this policy must record any information created or received in the course of daily business/transaction in official Council repositories.

4.2. Use of information

All those covered by the application of this policy **must** use and manage information appropriately, in accordance with Council's procedures whilst carrying out Council business and transactions.

All those covered by the application of this policy must ensure that all information that supports the business of Council is collected and created for **specified** purposes and that the reasons for collection and creation are transparent.

4.3. Using official repositories

Council information should only be created/received and managed in official Council repositories and business systems, which are appropriate to the format and context of the information. Employees should not create their own filing systems, or inaccessible repositories for Council information. All those covered by the application of this policy will be held accountable for managing information in the correct repository.

4.4. Information Disposal

Information disposal will be carried out in accordance with an approved Disposal Schedule as required by the Public Records Act 2005 [and signed off by the Chief Executive](#). Disposal of information must be carried out [as per this schedule](#), following audited disposal procedures under the guidance of the Programme Leader, [Information Management](#).

Destruction/deletion of Council information must only happen in a managed and approved manner, in accordance with Council's approved Disposal Schedule. All those covered by the application of this policy are not to destroy records that they deem as obsolete or paper copies of documents that have been scanned. Permanent destruction/deletion of any Council records is only permitted under the advice of the IM Programme Leader.

A record of all authorised disposals will be maintained by the Information Management Team.

4.5. Compliance with IM Policies

Failure to comply with Information Management policies could result in disciplinary action as detailed in the Council's HR13 Code of Conduct.

5. Approval

Current version approver name and position

Authorised by

Steve Manners

Group Manager – Information Science and Technology



Date of approval:

08/09/2022

Date Version Approved	Change Details	Officer sign-off
19/11/19	Initial Policy Approval	Chief Executive
08/09/2022	Minor Changes	Group Manager- Information, Science and Technology.