Privacy Policy

ORGANISATIONAL POLICY

POLICY REFERENCES

• Sponsor:	**Chief Operating Officer**
• Effective date:	April 2024
• Internal review due:	April 2027
• Legal compliance:	Privacy Act 2020 Building Act 2004 Local Government Act 2002 Local Government Official Information and Meetings Act 1987 Resource Management Act 1991 Public Records Act 2005
• Internal documents	Privacy Breach Response Plan Staff Code of Conduct Complaints Policy Information Management Policy Information Lifecycle Management Policy Information Security and Access Policy Cybersecurity Policy Protected Disclosures Policy Requests under the LGOIMA Policy
• Associated Documents/References	Archives New Zealand Information and records management standard
• Policy Number	CS24
• Approved by	Chief Executive

Contents

1. Purpose

1.1. The Council acknowledges that the responsible handling of personal information is not only a legislative obligation but is a key aspect of good corporate governance and maintaining community confidence in Council's delivery of services.

1.2. This policy outlines:

- the Council's obligations under the Privacy Act 2020.
- how the Council should collect, use, disclose, and store personal information,

2. Definitions

The **Council** is Tasman District Council.

Personal information is defined in section 7(1) of the Privacy Act 2020 as information about an identifiable individual. This may include, but is not limited to, information about an individual's:

- identity such as their name, marital status, title, date of birth and gender.
- contact details such as their address, email address and telephone numbers.
- financial details such as bank account and payment card details.
- correspondence with Council including transaction and interaction details such as information about payments to and from Council and other details of services they have requested or complaints made.
- technical information such as internet protocol (IP) address, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices they use to access our websites.
- profile information such as requests they have made, their feedback and survey responses.
- usage information such as information about how they use the Council's website, facilities and services.

The **Privacy Act** is the Privacy Act 2020.

A **third party** is an organisation or person who is not the Council.

3. Application

3.1. This policy applies to all employees, elected members and contractors of the Council.

3.2. This policy covers all personal information held by the Council and includes information collected:

- directly from an individual or third party.
- regardless of its format. This includes information collected on forms, in person, in correspondence, over the telephone or via the Council's website.

4. General principles

4.1. The Council should only collect personal information for the purpose of carrying out its functions and associated activities.

4.2. In summary, the Council's main functions and activities are:

- Public health and safety including monitoring public health; buildings; environmental health; liquor licensing and food safety; hazardous substances; animal control; civil defence and emergency management; parking control; and maritime safety.
- Transportation, roads and footpaths including managing the transportation network and associated assets.
- Environmental management including maintaining and enhancing biodiversity by monitoring resources, minimising inappropriate practices and managing pests.
- River and coastal asset management including promoting soil conservation; mitigating damage caused by floods and riverbank erosion; and maintaining and improving river assets. Council also owns and maintains wharves; jetties; boat ramps; associated buildings; foreshore protection walls; and navigational aids to support the safe use of coastal waters.
- Water supply including looking after the water supply schemes; managing the Wai-iti storage dam; and as a majority shareholder in the Waimea Community Dam.
- Wastewater collection, treatment, and disposal.
- Stormwater collection, reticulation, and discharge systems including drainage channels; piped reticulation networks; tide gates; detention or ponding areas; inlet structures; discharge structures; and quality treatment assets.
- Waste management and minimisation including curbside recycling and waste collection services; a materials recovery facility to process recycling; Resource Recovery Centres and transport services; and waste minimisation initiatives.
- Community development including operating parks and reserves; cemeteries; playgrounds; public toilets; libraries; community centres; an aquatic centre; community halls; museums; outdoor swimming pools; community housing complexes; community events; grant funding; and facilitating partnerships.
- Council enterprises including managing a commercial plantation forest; a mixture of leased and managed holiday parks; Port Tarakohe; Māpua wharf; and various other commercial property assets.
- Support services including customer services; communications; strategic policy; property; finance; human resources; information services; records management; and health and safety.

4.3. The Council should use, disclose and hold the personal information it collects in accordance with the Privacy Act 2020, and the Information Privacy Principles (see **Appendix A**).

4.4. The Council should take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure.

4.5. The Council should provide individuals with reasonable access to their personal information and take reasonable steps to correct such information when requested by that person, in order to ensure that records are accurate.

4.6. The Council should retain, store and dispose of personal information in accordance with the requirements of the Public Records Act 2005, associated Archives New Zealand Information and records management standard and the Council's information management policies.

5. Collection of personal information

5.1. The Council should only collect personal information necessary for it to fulfil a lawful purpose that is connected to one of its functions or activities.

5.2. The Council should collect personal information directly from the individual it is about, where possible. However, we may also collect information about an individual from a third party or a publicly available source.

5.3. When collecting personal information, the Council should take reasonable steps to advise that individual of the information being sought; for what purpose(s) it is being collected; whether any law requires the collection of the information; how the individual can contact the Council; and the main consequences, if any, of not providing the information.

6. Use and disclosure of personal information

6.1. The Council should use and share personal information to carry out its functions and activities. Generally, the Council should only use and share personal information for the purpose for which it was collected. In some cases, the Council may also use or share personal information for a directly related purpose or with the relevant individual's consent.

6.2. Purposes for which personal information may be used includes, but is not limited to:

- any specific purpose the individual is notified of at the time the personal information is collected.
- to provide services or facilities as requested.
- to positively confirm an individual's identity. This is to avoid inappropriate release or use of personal information.
- to respond to requests, enquiries, feedback, or other correspondence, or to contact an individual where it is necessary to resolve issues relating to Council services.
- to process an application for a consent, licence, registration, approval, permit, or other authorisation for which an individual has applied.
- to process an application to use or to register for any of our services or facilities, including online services.
- to process payments received by or made by the Council.
- to supply individuals with information about the Council and Council Controlled Organisations' (CCOs) events, news, services, or facilities that may be of interest.
- to enable the Council to undertake its law enforcement functions.
- to comply with relevant laws and regulations.
- to aid community safety.
- to carry out activities connected with the running of Council business or operations such as general administration, personnel training or testing, and maintenance of computer and other systems.

- as part of our commitment to customer service, to carry out surveys to improve our business processes and operations based upon feedback.

6.3. The Council may share personal information with:

- any person engaged by the Council to provide products or services to individuals on its behalf, where the personal information is necessary for the provision of those products or services.
- CCOs in order to assist with the functions and services that they provide on behalf of the Council.
- third parties if required to do so under any laws or regulations, including to comply with the Council's obligations under the Local Government Official Information and Meetings Act 1987, Building Act 2004 and Resource Management Act 1991.
- third parties during an investigation or defence of legal claims against the Council. This may include the Councils solicitors, consultants and investigators.
- third parties during an investigation or prosecution undertaken as part of the Council's law enforcement function. This may include New Zealand Police or other public sector agencies where criminal activity is reported or suspected. New Zealand Police may also access certain CCTV cameras from time to time, for law enforcement, investigation, and emergency response purposes.
- emergency services and other third parties where the Council believes it is necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual.
- any third parties that an individual authorises the Council to disclose their personal information to.
- any third party, if that information is held in a public register. This includes, but is not limited to, information collected in accordance with:
    - the Building Act 2004 which requires the Council to maintain a property file about each property in the District and makes this available to the public.
    - the Resource Management Act 1991 which requires the Council to make copies of resource consent applications available to the public.
    - the Local Government (Rating) Act 2002 which requires the Council to make our "complete rating information database" available to the public.
    - the Local Electoral Act 2001 which requires the Council to make the local electoral roll available for inspection in certain circumstances.
    - the Local Government Act 2002 which requires that the Council usually makes all submissions made during a special consultative procedure or other consultative procedure (for example submissions on proposed bylaws and the long-term plan) available to the public.
    - the Dog Control Act 1996 which requires the Council to maintain a register of all dogs and makes this information available in certain circumstances.
    - the Sale and Supply of Alcohol Act 2012 which requires the Council to maintain a register of license information and managers' certificates and makes this available to the public.

- the Reserves Act 1977 which requires the Council to make 'records of title' available to the public.

- third parties contracted by the Council to provide data hosting services and who may be based in other countries such as Australia or the USA. Appropriate safeguards should be put in place to ensure adequate protection of information.

6.4. Council should only disclose personal information to third parties outside New Zealand, excluding data hosting services, if the receiving third party:

- is subject to the Privacy Act 2020 because they do business in New Zealand, or
- will adequately protect the information, e.g. by using model contract clauses, or
- is subject to privacy laws that provide comparable safeguards to the Privacy Act 2020.

7. Storage and security of personal information

7.1. The Council should use a combination of people, process and technology safeguards across information, ICT, personnel and physical security to protect personal information from loss, and unauthorised access, use, modification and disclosure.

7.2. If the Council becomes aware of a privacy breach, Council should manage the breach in accordance with Council's Privacy Breach Response Plan.

7.3. Personal information should only be held by the Council for as long as is administratively necessary or required by law and should be disposed of in accordance with the requirements of the Public Records Act 2005 and relevant retention and disposal authorities.

7.4. Personal information should be destroyed or permanently de-identified when it is no longer required. In some cases, the Council is required to retain personal information indefinitely if it forms part of a 'protected record' under the Public Records Act 2005.

8. Accuracy and correction of personal information

8.1. Prior to using or sharing personal information, the Council should take all reasonable steps to ensure that it is accurate, up to date, complete, relevant, and not misleading.

8.2. Individuals may request changes to their personal information if they believe that it is inaccurate. If the Council agrees with this assessment, the personal information will be corrected. If the Council does not agree that the personal information needs to be corrected, a note of the request may be left on the disputed information as a 'statement of correction'.

9. Access to personal information

9.1. Individuals may request access their personal information held by the Council.

9.2. If an individual requests access to their personal information, the Council should take steps to confirm their identity. This may involve asking security questions and checking identity documents. Upon confirmation of an individual's identity, the Council should provide access to their personal information unless there are grounds to refuse access under the Privacy Act.

10. Refusal to provide personal information

10.1. If an individual refuses to provide personal information requested, the Council may not be able to adequately respond to their correspondence; process applications they have submitted; provide the services or facilities requested; process payments; or otherwise deal with any requests or enquiries they have submitted. If this occurs, the Council should explain why the personal information is required and the potential consequences of withholding it to the individual.

10.2. There are some circumstances where failure to provide personal information when requested may be unlawful or result in legal consequences. In these circumstances, the Council should explain why the personal information is required and the potential consequences of withholding it to the individual.

11. Responsibilities

11.1. As is required under section 201 of the Privacy Act, the Council should ensure that at least one employee is appointed as a Privacy Officer. However, responsibilities under the Act sit with the whole of Council.

11.2. The Privacy Officer(s) will be responsible for assisting the Executive Leadership Team to encourage organisational compliance with the Information Privacy Principles; overseeing requests and complaints made under the Privacy Act and enquiries and investigations by the Privacy Commissioner; and assisting the Executive Leadership Team to ensure that the Council complies with the provisions of the Privacy Act.

11.3. All managers are expected to understand, effectively implement, support and demonstrate a positive commitment to this policy.

11.4. All employees are expected to read and understand this policy and ensure that personal information is collected and handled in a responsible manner, in accordance with the Privacy Act.

12. Non-compliance with this policy

12.1. If a Council employee fails to comply with this policy, disciplinary action may be taken in accordance with the Code of Conduct.

13. Privacy complaints

13.1. Individuals may contact the Privacy Officer(s) at any time to enquire about Council's privacy practices, raise concerns, or make a complaint about the way the Council has handled their personal information.

13.2. If an individual is not satisfied with the way the Council has handled their complaint, the Privacy Officer(s) will advise them of their right to go to the Privacy Commissioner for assistance or to make a complaint.

Authorised by Leonie Rae - CEO

Date of approval: 1 April 2024

Appendix A

The Privacy Act includes 13 Information Privacy Principles which the Council is required to comply with. These principles are outlined below:

Information Policy Principles from the Privacy Act 2020
Principle One
The Council must only collect personal information if it is for a lawful purpose connected with our functions or activities, and the information is necessary for that purpose.
Principle Two
Personal information should be collected directly from the person it is about. The Council may collect personal information from other people in certain situations. For instance: • if the person concerned authorises collection from someone else, • if the information is collected from a publicly available source, • if collecting information from the person directly is not really practicable or would undermine the purpose of collection.
Principle Three
The Council should be open about why we are collecting personal information and what we will do with it. When the Council collects personal information, we must take reasonable steps to make sure that the individual knows: • why it's being collected, • who will receive it, • whether giving it is compulsory or voluntary, • what will happen if the information isn't provided.
Principle Four
The Council must collect personal information in a way that is lawful and seen as fair and reasonable in the circumstances.

Information Policy Principles from the Privacy Act 2020
If we break the law when collecting information, then we have collected information unlawfully. What is fair also depends on the circumstances such as the purpose for collection, the degree to which the collection intrudes on privacy, and the time and place it was collected. The Council needs to take particular care when collecting information from children and young people. It may not be fair to collect information from children in the same manner as we would from an adult.
Principle Five
The Council must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information. If the Council has a serious privacy breach, we must notify the Office of the Privacy Commissioner as soon as possible (within 72 hours).
Principle Six
Generally, the Council must provide access to the personal information we hold about someone if the individual in question asks to see it. In some situations, we may have a good reason to refuse a request for access to personal information. For example, the information may involve an unwarranted breach of someone else's privacy or releasing it may pose a serious threat to someone's safety.
Principle Seven
Individuals have a right to ask the Council to correct information about them if they think it is wrong. If the Council does not agree that the information needs correcting, the individual can ask that we attach a statement of correction to its records, and we should take reasonable steps to do so.
Principle Eight
The Council must check that personal information is accurate, up to date, complete, relevant and not misleading before it is used or disclosed.
Principle Nine
The Council should not keep personal information for longer than it is required for the purpose it can lawfully be used.
Principle Ten
The Council can generally only use personal information for the purpose it was collected, and there are limits using personal information for different purposes. Sometimes other uses are allowed, such as use that is directly related to the original purpose, or if the individual gives their permission for their information to be used in a different way.
Principle Eleven
The Council may generally only disclose personal information for the purpose for which it was originally collected. Sometimes other reasons for disclosure are allowed, such as disclosure for a directly related purpose, or if the person in question gives their permission for the disclosure. For instance, we may disclose personal information when: ▪ disclosure is one of the purposes for which the Council got the information, ▪ the individual concerned authorises the disclosure, ▪ the information is to be used in a way that does not identify the individual concerned, ▪ disclosure is necessary to avoid endangering someone's health or safety, ▪ disclosure is necessary to uphold or enforce the law.
Principle Twelve
The Council may only disclose personal information to another organisation outside New Zealand if we check that the receiving organisation: ▪ is subject to the Privacy Act because they do business in New Zealand,

Information Policy Principles from the Privacy Act 2020

- will adequately protect the information, or
- is subject to privacy laws that provide comparable safeguards to the Privacy Act.

If none of the above criteria apply, we may only make a cross-border disclosure with the permission of the individual concerned. The individual must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

Principle Thirteen

The Council can only assign unique identifiers to individuals when it is necessary for our functions.
Unique identifiers are individual numbers, references, or other forms of identification allocated to people by organisations as a way to uniquely identify the person to the organisation assigning the identifier. Examples include drivers license numbers, passport numbers, IRD numbers, or National Health Index (NHI) numbers.
The Council cannot assign a unique identifier to an individual if that unique identifier has already been given to that person by another organisation.
The Council can record (and use) an individual's unique identifier so that we can communicate with another organisation about the individual.
The Council must also take reasonable steps to protect unique identifiers from misuse and make sure we verify someone's identity before assigning a unique identifier.