The Waimakariri District Council will hold a Workshop Session in the Council Chambers,

Rangiora Service Centre, 215 High Street, Rangiora, on

Tuesday, 21 April 2026, from 9.30am to 10am

This Briefing Session is a non-decision-making meeting.

Workshop Sessions are open to the public and are therefore advertised. However, Briefing Sessions are public excluded.

AGENDA

Time	Workshop or Briefing	Details	Pre-reading Material	Next Action
9.30am to 10am *(30min)* *10 min (Pres)* *20 min (Q & A)*	***Workshop***	***CCTV & Other Recording Devices Policy –*** *S Docherty and K Brocas* ***Purpose:*** *To present a new policy which aligns the Council's handling of recorded information with the Privacy Act 2000. The Policy applies to data that is video-only, audio-only, or video and audio combined, and that is collected by the Council through different technologies. The Policy ensures that the purposes for the collection, storage, and deletion of private information align with the requirements of the Privacy Act.*	*Attachments A and B*	*Report to Council*
11.15am to 11.30am *(15min)*	***Briefing***	***Update from the Chief Executive***		

Waimakariri District Council
215 High Street
Private Bag 1005
Rangiora 7440, New Zealand
Phone 0800 965 468

Closed Circuit Television (CCTV) and Other Recording Devices Policy

1. Introduction

Waimakariri District Council (WDC) owns, operates and manages devices capable of recording information in the Waimakariri District. WDC must comply with the provisions of the Privacy Act 2020 and the Local Government Official Information and Meetings Act 1997 (LGOIMA) in the collection, dissemination, storage and removal of personal information, and this policy follows best practice in relation to individual's rights to privacy in accordance with the Privacy Act 2020.

2. Policy Context

WDC, in operating recording devices, will maintain the protection of individuals' privacy by:

- ensuring information is collected for necessary and lawful purposes only
- taking reasonable steps to make individuals aware that information is being collected and the reason for such collection
- ensuring that information is collected in a fair manner
- ensuring the appropriate management and security of recorded information
- ensuring information is used only for the purpose for which it was collected
- complying with Principles 6, 9 and 11 of the Privacy Act relating to access to and retention and disclosure of information.

3. Policy Objective

This Policy sets out the purpose for collecting audio and visual recordings, how the information is collected, how long it is retained and how the privacy impacts will be minimised. Access to Council recorded information is limited and controlled by the WDC.

This policy applies to all Council employees, contractors to Council, councillors, the New Zealand Police (Police) and the general public who may access areas where recording devices may be operating.

4. Policy Statement

4.1. Purpose of collection of personal information

4.1.1. The WDC operates or facilitates recording devices to support public and staff safety on Council property, facilitate regulatory enforcement and support the closed-circuit television network that is utilised by the Police. These purposes align with Principle 1 of the Privacy Act 2020, specifically:

- Personal information is connected with the function or activity of the agency; and

- The collection of the information is necessary for that purpose.

4.1.2. The WDC Privacy Policy is located on the WDC website and is available in hardcopy by request. This Policy sets out the following:

- General notice that information is being collected
- The purpose/s of that information being collected
- Advising other external agencies may access the information collected

4.2. CCTV Recording

4.2.1. WDC facilitates or operates CCTV in locations for the following purposes:

- Crime Prevention Through Environmental Design (CPTED)
- Community-led initiatives involving government agencies, social service agencies, businesses and community groups or volunteers
- To provide a security presence during seasonal/short term issues
- Compliance and enforcement of bylaws, resource consent conditions and legislation
- Managing traffic and monitoring traffic movements in particular areas
- Enhancing public safety and community wellbeing by deterring and preventing criminal and antisocial behaviour in public places throughout the district, including for the protection of public assets from acts of vandalism

4.2.2. Signage notifying that CCTV is operating within public buildings is displayed in a prominent position. The sign should be prominent enough to advise the public that cameras are operating before they are close enough to be filmed.

4.2.3. Only authorised people will be able to watch the CCTV footage for the purposes mentioned above or to regularly check the system is working. We will not actively attempt to identify individuals from the CCTV footage unless a reported or suspected incident needs investigation.

4.2.4. WDC does not accept ownership or operational control over any vested cameras from third parties.

4.3. Live streaming and recording of meetings and ceremonies

4.3.1. In the interests of making our decision-making process transparent and accessible, public Council meetings are broadcast live online and then made available on our website.

4.3.2. Meetings that are being filmed will be signposted clearly stating they are filmed at the entry into the meeting room. Most of the filming will cover elected members as they speak and debate at the meeting, however, the filming may also include members of the public in the background and of anyone speaking at a public forum. The footage will be publicly available and can be accessed from our website.

4.3.3. Photos or video footage may be recorded by WDC at civic events in Waimakariri (e.g. citizenship ceremonies and other public or community events that we manage) for internal or external publications. Signage on display or other communication at an event will let members of the public know if photography or filming will be taking place. Members of the public who do not want to be included in any photos or video footage may request this of our staff members present at the event.

4.4. Body worn cameras

4.4.1. Cameras are worn by our compliance officers as a deterrent to anti-social behaviour towards them and to provide a clear record of events if an altercation occurs. The officer

will only start recording if an interaction escalates and will notify those present when the recording device is activated.

4.4.2. When inside a building where public are excluded or within a private property the compliance officer will inform that footage is being recorded and gain consent at the time.

4.4.3. When in a publicly accessible space, or outside of a building, the compliance officer will inform those present of the recording device in situations where it is safe to do so.

4.4.4. Body-worn cameras are always recording but do not store the information until activated. The only time this footage is stored is if a staff member activates their camera. The last 30 seconds of video is clipped to the recording to add context to the video (e.g. how a situation unfolded prior to the staff member pressing record).

4.4.5. All authorised staff who are equipped with body worn cameras are also equipped with appropriate signage on their uniform to indicate an audio and visual recording device is being worn at that time.

4.5. Audio only recording devices

4.5.1. Audio only recording devices may be used for the purposes of regulatory enforcement. In circumstances where audio monitoring devices are to be used on a property, the informed written consent of the homeowner will be obtained prior to placing the device within their property.

4.5.2. Placement of the device will be made in a way that minimises the incidence of inadvertently collecting other audio and will be within the boundaries of the property that has given permission to record.

4.6. Request for official Information from the public

4.6.1. LGOIMA provides for people to make a request for official information held by government agencies. Any person may make a request for information held by WDC.

4.6.2. Official information requests for CCTV images made under LGOIMA will be processed by the Governance team and managed in accordance with section 7 of LGOIMA.

4.6.3. If CCTV footage is requested because of an incident or alleged crime, the first point of contact is the local Police who can request the footage

4.7. Requests by WDC staff for release of footage

4.7.1. Internal requests made by WDC staff shall be made using the footage request form available on the WDC intranet. Requests for footage require approval from the General Manager of the department requesting the footage. Release of the footage is at the discretion of the *nominated person/s*

4.7.2. Internal requests for camera footage must:

4.7.2.1. Be recorded in the WDC's information management system

4.7.2.2. The use of the information must be for the purpose that it was collected

4.7.2.3. Is subject to the provisions of the Privacy Act 2020

4.7.3. All internal requests for footage will be reported to the *nominated persons/business unit* and will include the requestors details, the authoriser's name, the reason for accessing the data and the period and location covered by the footage.

4.7.4. Each time the footage is accessed it will be recorded electronically in a log, including access by Elected Members, individuals and the Police. This log will be presented at the

nominated persons/business unit for review.

4.8. New Zealand Police and other agencies

4.8.1. WDC undertakes to cooperate and assist the New Zealand Police (Police) where requests for footage are made and are justifiable. Should a member of the public request footage relating to a criminal matter, this will be referred to Police who may, at their discretion, request the footage, complying with the provisions of the Privacy Act 2020.

4.8.2. WDC makes its properties available for Police and Waka Kotahi to install monitored CCTV equipment. These cameras are owned and operated by the Police and WDC does not have access to this footage.

4.9. Retention and disposal of recorded information

4.9.1. Video and audio will be recorded and retained on secure servers for a period of up to 90 days from recording. All footage will remain the property of WDC during this time until it is erased in line with this Policy. Servers and technology containing recorded footage are housed in a secure location and accessible only by those authorised personnel only. A record of those personnel is held and maintained by the Privacy Officer.

4.9.2. The only exception to the 90-day retention period is where an incident of a serious or potentially serious nature has been captured on the footage. Retention of the footage will be used for investigation or resolution of the incident, or for use by the Police or potential legal proceedings.

4.9.3. Written permission of the Privacy Officer is required for partial retention of the footage over and above the 90-day period.

4.9.4. Public requests for images or footage relating to a criminal matter will be referred to the Police in the first instance.

5. Definitions

5.1. CCTV

5.1.1. In this policy, the phrase “CCTV” is used to mean any type of camera, recording device, or other related technology. It is recognised that CCTV is a legacy term, specific to an increasingly redundant technology. However, it is widely understood to refer to the types of surveillance and monitoring technologies with which this Policy is concerned.

6. Links to legislation and other policies

Legislation:

- Privacy Act 2020
- Local Government Official Information and Meetings Act 1987
- Health and Safety at Work Act 2015
- Local Government Act 2002

Other Policies:

- Privacy Policy
- Privacy Commissioners Guidance on CCTV

7. Questions

Any questions regarding this policy should be directed to the Position Title of Policy Owner in the first instance.

8. Relevant documents and legislation

9. Effective date

Date Month Year

10. Review date

Date Month Year

11. Policy owned by

Manager, Insert Department Name e.g. Regulation

12. Approval

Approved:
INSERT CHIEF EXECUTIVE'S
SIGNATURE IN PLACE OF THIS TEXT

Chief Executive
Waimakariri District Council

OR

Adopted by Waimakariri District Council on Date Month Year

TRIM / Quality Number – Version Number – Month Year

A quick tour of the privacy principles

The Privacy Act 2020 has 13 privacy principles that govern how you should collect, handle and use personal information.

1 You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

2 You should generally collect personal information directly from the person it is about. Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:

- the person concerned gives you permission
- collecting it in another way would not prejudice the person's interests
- collecting the information from the person directly would undermine the purpose of collection
- you are getting it from a publicly available source.

3 When you collect personal information, you must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if they don't give you the information.

Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

4 You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

5 You must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

6 People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:

- endanger someone's safety
- create a significant likelihood of serious harassment
- prevent the detection or investigation of a crime
- breach someone else's privacy.

Privacy Commissioner
Te Mana Mātāpono Matatapu

7 A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

8 Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

9 You must not keep personal information for longer than is necessary.

10 You can generally only use personal information for the purpose you collected it. You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

11 You may only disclose personal information in limited circumstances. For example, if:

- disclosure is one of the purposes for which you got the information
- the person concerned authorised the disclosure
- the information will be used in an anonymous way
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to avoid a prejudice to the maintenance of the law

12 You can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
- the information is going to a place with comparable privacy safeguards to New Zealand
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

13 A unique identifier is a number or code that identifies a person in your dealings with them, such as an IRD or driver's licence number. You can only assign your own unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation. If you assign a unique identifier to people, you must make sure that the risk of misuse (such as identity theft) is minimised.

Content updated January 2021. Design updated March 2025.