

COUNCIL POLICY

Surveillance Technology

Contents

1. Purpose.....	4
2. Scope.....	4
2.1 In scope	4
2.2 Outside of scope.....	4
3. Policy details	5
3.1 Context.....	5
3.1.1 Surveillance and privacy.....	5
3.1.2 Crime Prevention Through Environmental Design (CPTED)	5
3.1.3 Auditor General Report	5
3.1.4 Guiding Principles for Surveillance	6
3.2 Oversight and Management.....	7
3.2.1 Oversight.....	7
3.2.2 Management	8
3.2.3 Transitional Arrangements.....	9
3.3 Types of surveillance devices	9
3.3.1 Body Worn Cameras and Personal Duress Alarms	9
3.3.2 CCTV	10
3.3.3 Tourism cameras and photography	10
3.3.4 Asset Inspection Cameras	11
3.3.5 Location tracking devices and software	11
3.3.6 Other types of surveillance devices	11
3.4 Privacy and Data Protection	11
3.5 Access to surveillance device information.....	12
3.5.1 Internal Requests	12
3.5.2 External requests (non law enforcement agency).....	13
3.5.3 External requests (law enforcement agency).....	13
3.6 Discretion to act	13
4. Human Rights Charter compatibility	13
5. Gender Impact Assessment.....	13
6. Supporting documents.....	14
7. Definitions and abbreviations	14
8. Approval.....	16

DOCUMENT UNCONTROLLED WHEN PRINTED

Document Control		
Policy number 135	Status Adopted by Council	Approved by Council
Date approved: 30 June 2026	Next review date April 2030	
Directorate Corporate and Community	Department Corporate	External

REVISION RECORD

Date	Version	Revision description
9 April 2026	1.0	Draft for public exhibition
30 June 2026	2.0	Adopted

1. Purpose

The Surveillance Technology Policy provides a framework for all activities that involve recording images or audio that may have privacy implications and protects the rights of those whose images or details may be captured.

The Policy supports the Alpine Shire Council Plan 2025-2029 in the following areas:

- Strategic Direction 3 – Transparent and accountable leadership
- Objective 1 – Customer Focused Alpine, Priority 1.3, Major Initiatives 6 and 7
- Objective 3 – Vibrant and Health Alpine, Priority 3.5 and 3.8

2. Scope

2.1 IN SCOPE

The Policy applies to all Council employees, Councillors, contractors, tenants of Council facilities and volunteers who use cameras or audio recording equipment in the course of their work for a variety of purposes, with the common thread that the recording of images or audio has real, perceived or potential privacy issues. The Policy covers the following types of image / audio recordings:

- Body worn cameras
- Personal duress alarms
- Closed-Circuit Television (CCTV)
- Tourism cameras and marketing / promotional videos and photos
- Asset inspection cameras including drones and vehicle mounted cameras
- Location tracking technology such as vehicle GPS tracking or asset management software
- Other recording devices such as traffic survey cameras

The Policy is supported by procedures and Terms of Reference which cover the operational and administrative aspects of how Council uses the various types of cameras and recording devices outlined above.

2.2 OUTSIDE OF SCOPE

This policy does not cover the use of other types of technology or data capture for surveillance including facial recognition technology, artificial intelligence or data capture and analysis e.g. web browsing history or metadata.

Council records audio, still images or video for many purposes that may not have privacy or data protection implications, and as such are not required to be covered by this policy. This includes (for example) photos of defects or damage to Council assets, recording by Environmental Health staff undertaking food premise inspections, Statutory Planning staff taking photos to assist in documenting planning decisions, and many more instances that reflect a legitimate and proper purpose pursuant to Council's work, that do not impact on anyone's privacy by capturing personal information.

If there is any doubt about whether an activity is covered by this policy, officers should apply the surveillance principles if necessary and seek advice from the Surveillance Oversight Committee.

3. Policy details

3.1 CONTEXT

3.1.1 Surveillance and privacy

The concepts of privacy and what constitutes surveillance are relevant to ensure that this policy only regulates activities that fall within its scope. In general:

- Surveillance refers to the monitoring and analysis of data to collect information about individuals, groups or contexts, often through technology such as CCTV or Body Worn Cameras. Surveillance is regulated by the *Surveillance Devices Act 1999* (SD Act).
- Privacy is a broad concept and relates to the protection of personal information. This information is anything that is recorded about a person, including CCTV or Body Worn Camera footage and photographs. In practical terms, people may have a higher or lower expectation of privacy depending on the context, but any recording that enables a person to be identified must be treated as personal information and managed in accordance with the *Privacy and Data Protection Act 2014* (PDP Act).

Further information on surveillance and privacy are available on the Office of the Victorian Information Commissioner (OVIC) website.

3.1.2 Crime Prevention Through Environmental Design (CPTED)

The concept of Crime Prevention through Environmental Design (CPTED) is a holistic, multi-disciplinary approach based in urban design principles. CPTED Australia defines it as follows:

CPTED is a design philosophy that focuses on reducing opportunities for crime by modifying the physical environment. The idea is simple: when spaces are thoughtfully planned and well-managed, they can encourage positive behaviours and discourage anti-social ones.

Rather than responding to crime after it occurs, CPTED aims to prevent it from happening in the first place. It does this by making potential offenders feel exposed, unwelcome, or deterred — all through smart environmental design.

While surveillance can be a legitimate way to improve safety or protect assets, it may also act as a 'band aid' solution that does not tackle the underlying issues that cause the problem in the first place. Simple examples of CPTED include better lighting or improved sightlines to allow 'passive' or incidental surveillance of an area by passing pedestrians or surrounding residential properties.

In this regard, CPTED should be considered as a primary measure prior to the installation of surveillance devices. There are numerous readily available resources that provide further information and training on CPTED, including CPTED Australia (cpted.com.au).

3.1.3 Auditor General Report

The Victorian Auditor General (VAGO) conducted an audit of CCTV usage by five Victorian councils in 2018 (*Security and Privacy of Surveillance Technologies in public places*) and concluded that there are two fundamental requirements for effective CCTV usage by Councils:

1. Appropriate management and oversight of surveillance activities
2. Adherence to privacy and data protection requirements.

While focused on CCTV, the VAGO requirements are broadly applicable to all surveillance activities.

3.1.4 Guiding Principles for Surveillance

The Office of the Victorian Information Commissioner (OVIC) has created seven guiding principles for surveillance, to assist organisations that use surveillance to meet their privacy obligations under the PDP Act.

3.1.4.1 Principle 1: Legality

In order to ensure legality, Council will:

1. Ensure all surveillance is lawful, based on Information Privacy Principle 1.2, PDP Act.
2. Conduct a Privacy Impact Assessment prior to installing or using any surveillance device.
3. Comply with the Information Privacy Principles in the PDP Act when collecting personal or sensitive information through surveillance.
4. Periodically review its surveillance practices to ensure they remain lawful.

3.1.4.2 Principle 2: Legitimate Aim

1. Council will only collect personal information by surveillance if it is connected to a legitimate aim that directly corresponds to the organisation's functions or activities. In general, these aims fall under three potential categories:
 - a. Protection of the person
 - b. Protection of property
 - c. Protection of the public interest
2. Council will limit the use of any personal information collected through surveillance to the primary purpose of the surveillance, or a permitted secondary purpose.

3.1.4.3 Principle 3: Necessity

1. Council will limit personal information collected through surveillance to that which is necessary to achieve the aim (from Principle 2).
2. Council will not collect information through surveillance where it would be reasonable and practical to collect that information directly from the person without using surveillance.

3.1.4.4 Principle 4: Proportionality

Principle 4 is addressed if Council:

1. Assesses the proportionality of the surveillance required in the particular circumstances of an individual case, to ensure the surveillance is carried out in a way that is least likely to impact on privacy and human rights.
2. Limits surveillance to the least intrusive acts, practices, or methods that are necessary to achieve a legitimate and lawful aim.
3. Limits surveillance to relevant individuals only.

3.1.4.5 Principle 5: Safeguards

Council has implemented procedural safeguards for all surveillance activities and will ensure that these safeguards are properly resourced. This encompasses the following areas:

1. Transparency. Council will take reasonable steps to ensure that people whose personal information is collected through surveillance will be made aware of the surveillance, who has conducted it, the purpose, and how to contact Council to find out more information.
2. Anonymity. Council will only collect anonymous information through surveillance, rather than personal information, wherever it is reasonably practicable.
3. De-identification. Council will destroy or de-identify personal information collected through surveillance when it is no longer needed.
4. Information sharing. Council will not share information gathered through surveillance, unless the sharing is related to the purpose of the surveillance, or for another lawful purpose. Managing any requests to share information is covered in Section 3.5 of this policy.
5. Information security. Council will take reasonable steps to protect personal information collected through surveillance from being misused, lost, or accessed, disclosed or modified by unauthorised persons.
6. A Privacy Impact Assessment will be required for each application for surveillance technology.

3.1.4.6 Principle 6: Non-discrimination

Council will not use surveillance in any manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. A Gender Impact Assessment will be required for each application for surveillance technology.

3.1.4.7 Principle 7: Complaints and Remedy

1. Council will provide information and pathways for individuals to complain to Council where they believe their privacy has been unreasonably impacted.
2. Council will work constructively to remedy any complaints, including if they are escalated to the Victorian Information Commissioner.

3.2 OVERSIGHT AND MANAGEMENT

3.2.1 Oversight

Oversight and decision making relating to the Surveillance Technology Policy is governed by an internal Surveillance Oversight Committee ("the Committee").

The Committee will have its own Terms of Reference and will meet as required to oversee Council's surveillance technology operations and assess new applications or changes as needed.

The Committee is constituted by the CEO, and its membership is defined in the Terms of Reference.

The Committee provides a recommendation to the CEO on the installation, modification and use of all surveillance technology. The CEO is the approver of all decisions relating to surveillance technology, except for the installation or modification of Category 1 CCTV systems.

Category 1 CCTV systems must be approved by Council following a recommendation from the Committee, unless they relate to modifications which are deemed to be minor operational changes by the CEO.

The operations and functions of the Committee are detailed in the Terms of Reference.

3.2.2 Management

The roles and responsibilities for the operation of the policy are detailed in the following table. In the event that officer titles change over the life of the policy, the CEO may designate a new officer responsible for the tasks below.

Task	Responsible
Overall responsible for Surveillance Technology Policy	Manager Corporate
Making decisions on the installation and management of Category 1 CCTV systems	Council
Making decisions on the installation and management of all other surveillance technology described in this policy	CEO
Making recommendations on the installation and management of all other surveillance technology described in this policy	Surveillance Oversight Committee
Responsible for storage, access and deletion of data in accordance with data privacy requirements	ICT Coordinator, tenant or private contractor
Inclusion of appropriate clauses in leases / licenses with tenants who wish to install or modify a Category 3 CCTV system	Property and Contracts Coordinator
Inclusion of appropriate agreements for any external providers who manage surveillance data on behalf of Council	ICT Coordinator
Maintaining a list of approved surveillance technology systems / devices (all categories)	Surveillance Oversight Committee
Decisions related to releasing or viewing footage, images or audio, including for FOI requests	Manager Corporate
Developing supporting administrative procedures and templates, e.g. Privacy Impact Assessment, Surveillance Technology Request Procedure	Manager Corporate

Task	Responsible
Developing site specific operating procedures	Manager responsible for location or facility
Preparing requests for new or changes to Surveillance systems (Surveillance Technology Request Procedure)	Manager responsible for location or facility

3.2.3 Transitional Arrangements

The Policy includes a transitional period of one year from the date of adoption, during which time all existing surveillance technology used by Council will be assessed by the Surveillance Oversight Committee and brought up to the standard stipulated by this policy (if required).

3.3 TYPES OF SURVEILLANCE DEVICES

3.3.1 Body Worn Cameras and Personal Duress Alarms

3.3.1.1 Purpose

Body Worn Cameras (BWC) and Personal Duress Alarms are used by Council staff to promote and maintain a safe working environment. BWC are also used to record conversations or incidents related to investigating breaches of acts, regulations or laws, or for recording conversations or events for later reference with consent of all involved parties.

3.3.1.2 Authorisation

Staff must be authorised by the CEO, based on a recommendation from the Surveillance Oversight Committee to use BWC or Personal Duress Alarms.

3.3.1.3 Activation

Staff using BWC and Personal Duress Alarms must activate their device in any the following circumstances, if it is safe to do so:

- Where there is a reasonable concern for the safety of any person
- To gather evidence of a breach of an Act, legislation or law that Council is responsible for
- For training purposes, with the consent of parties whose image or audio may be captured

In addition, BWC may be activated with the consent of all affected parties where deemed necessary or useful in recording conversations or events for later reference.

Prior to recording, or as soon as practicable the staff member is to inform any person in the vicinity of the recording, if it is safe to do so and it is likely that a private conversation may be captured. In public spaces where there is no immediate likelihood of recording a private conversation, the staff member may inform of the recording at their own discretion.

3.3.2 CCTV

CCTV falls into four categories. Applications for CCTV need to consider the guiding principles for surveillance.

3.3.2.1 Category 1

Council operated CCTV systems that are installed in public places that Council manages (such as local streets, public car parks or public reserves) that are intended to enhance community safety and detect criminal behaviour such as vandalism. Footage from these cameras can be made available to relevant authorities under whose jurisdiction any offence falls. For example, evidence of vandalism could be provided to Victoria Police, whereas evidence of rubbish dumping could be provided to Council's Local Laws Officers, following the process detailed in Section 3.5 of this Policy.

3.3.2.2 Category 2

Council has a range of CCTV facilities at public facilities. These are primarily for the protection of assets and protection of public or staff safety. In addition, the CCTV in Council Chambers is used to record Council Meetings, which relates to protection of the public interest.

3.3.2.3 Category 3

CCTV is used in some instances by tenants of Council facilities, for example at sports and aquatic facilities. In this instance, the CCTV must be justified in the same way as for a Category 2 facility, and a written agreement put in place to ensure that the tenant complies with the relevant privacy and data storage / access requirements.

3.3.2.4 Category 4

Category 4 CCTV systems are temporary devices such as movement activated trail cameras. They can be used by Council's Compliance team to detect, deter or investigate matters that fall under Council's jurisdiction, such as dumping of rubbish on Council land. The use of these systems is similar to Category 1 or 2, except that they are temporary in nature.

3.3.3 Tourism cameras and photography

Council uses photography and video for tourism / events related promotion and marketing. These uses are not for the purpose of surveillance but may capture private information about individuals. They fall into two categories:

- Marketing / promotion photos and video. Photos and / or video taken for marketing purposes, for example of an event. Written permission must be sought for any person captured who is identifiable, including permission for the photo / video to be used for marketing / promotional purposes. The procedure and waivers for these types of photo / video must be approved by the Committee.
- Web cameras. Council operates tourism cameras at Dinner Plain, which display images of the ski slope that are available live on the Dinner Plain web page. The intent of these cameras is to provide information about snow conditions to people prior to travelling to Dinner Plain, not surveillance. However, there is a chance that a person could be identified by the cameras, and while the footage is not recorded it would be possible to capture images from the web page.

Decisions regarding the installation, modification and the operation of the tourism cameras is within the scope of the Committee.

3.3.4 Asset Inspection Cameras

Council records photos and videos for the purpose of recording and tracking the condition of assets. This may include vehicle mounted cameras (used for purposes such as road / footpath audits), taking photos by staff and using other technology such as drones fitted with cameras. In general, the purpose of collecting images and footage does not fall within the definition of surveillance, unless it can identify people or captures private space.

As such, the Committee may give a standing approval for such recording, on the condition that a Surveillance Technology Request Procedure is submitted to the Committee for consideration, detailing all types of proposed recording and the potential privacy risks and how these will be mitigated. Types of mitigation may include:

- Efforts are made to avoid capturing any personal details or private space (for example by angling cameras down to only capture the footpath or road)
- Signage is used to notify of the use of recording devices in the area (can be mounted on the vehicle or static signage)
- Permission is gained from any potentially impacted person (e.g. inadvertent video capture of a private backyard by a drone may require permission)

Staff involved in the use of asset inspection cameras / recording devices are to be familiar with the privacy requirements of this policy.

3.3.5 Location tracking devices and software

Council may use location finding software and devices in Council vehicles, devices (such as Body Worn Cameras and Personal Duress Alarms) and as part of software (for example asset management software and job tracking software). The information collected from these devices can be used for staff safety, fraud control and workflow management. All staff who may be subject of such technology are to be made aware that it is in place.

3.3.6 Other types of surveillance devices

Council may also use (or engage a third party to use) other types of devices that have the potential to be surveillance devices. This may include technology such as traffic survey cameras or externally conducted drone surveys.

Such uses may not require a decision of the Committee, but the person responsible for managing the activity must satisfy themselves that relevant privacy and data protection standards will be met, or that there are no relevant privacy / data protection issues. If there is any doubt, the matter can be referred to the Committee for consideration.

3.4 PRIVACY AND DATA PROTECTION

Footage, images or audio collected by surveillance devices will be treated by Council in full compliance with the *Privacy and Data Protection Act 2014* ("PDP Act"). In practical terms, this means that the footage will be stored securely, and access will only be granted to view the footage for a legitimate purpose, such as investigating an alleged offence, injury or safety breach.

A Privacy Impact Assessment will be required for each application for surveillance technology, and assessed accordingly by the Surveillance Oversight Committee.

Where tenants of Council facilities have their own CCTV installed, a written agreement will be made (whether as part of the lease / license or as a separate agreement) to ensure that the CCTV device is operated consistently with the requirements of the PDP Act, and footage is only accessed for a legitimate purpose.

If Council engages third party providers of surveillance services, a written agreement is to be made as part of contract documentation to ensure compliance with the PDP Act.

Council's Governance Officer will provide advice to the Committee and operators of surveillance technology systems or others acting under the Policy of their requirements to comply with the PDP Act.

Affected Council staff will be consulted with prior to the installation of CCTV systems in any workplace. Where possible, staff preferences relating to CCTV installation will be taken into account. However, in making a decision, the Committee must take into account all relevant considerations, including staff safety, the likelihood of any criminal activity, or the requirement for protection of assets.

Signage will be installed for all types of surveillance devices except BWC and personal duress alarms.

Footage and other data will be deleted when it is deemed to no longer be required, usually within 28 days.

3.5 ACCESS TO SURVEILLANCE DEVICE INFORMATION

Requests for access to images, audio or video footage for which Council is responsible, and where data is stored falls into three categories.

3.5.1 Internal Requests

Internal requests are from appropriate staff to access images, audio or video footage. These requests are to be assessed by the chair of the Surveillance Oversight Committee, who will assess whether the release is appropriate.

Only staff involved in an investigation of a suspected incident would be permitted to view footage to conduct an investigation or to confirm if it is appropriate to hand over to an investigative body (e.g. Victoria Police, WorkSafe Victoria).

Staff that may request access to recorded images, audio or video footage may include:

- CEO
- Directors
- Managers
- Compliance Coordinator
- Local Laws Officers
- Building Surveyor
- Environmental Health Officer
- Maternal and Child Health Nurses
- Other staff members authorised in writing by the CEO

Standing approvals may be granted in certain circumstances, for example where staff are monitoring Category 4 CCTV cameras for illegal behaviours or the routine use of BWC footage to accurately record conversations or events for later reference.

3.5.2 External requests (non law enforcement agency)

Requests for access to images, audio or video footage by external parties are via an FOI request. Such requests will be assessed by the normal FOI process. Where material is released through this process it would have any personal information redacted (e.g. by blurring faces or number plates in video or photos).

3.5.3 External requests (law enforcement agency)

Law enforcement requests for surveillance images, audio or video footage will be dealt with pursuant to the provisions of the Privacy and Data Protection Act 2014, i.e. access will be approved where Council is satisfied that the request is for a valid law enforcement purpose. These requests will be assessed by the chair of the Surveillance Oversight Committee.

Any decision to release images, audio or video footage under this provision requires written documentation from the party requesting the footage and a Council record of who the data was provided to and the justification.

3.6 DISCRETION TO ACT

The Chief Executive Officer may exercise discretion and make decisions under circumstances not directly covered by this CCTV Policy as long as Council's legal obligations are met.

4. Human Rights Charter compatibility

While surveillance can impact on human rights including people's privacy, if it is managed in accordance with this policy it has been assessed as being compatible with the *Charter of Human Rights and Responsibilities Act 2006 [Vic]*.

5. Gender Impact Assessment

The implications of this policy were assessed in accordance with the requirements of the Gender Equality Act 2020. The Gender Impact Assessment found that surveillance activity has the potential for both positive and negative impacts, to a range of groups including culturally and linguistically diverse people, vulnerable community members, indigenous people and women.

These impacts could include:

- Positive impacts, particularly for women, due to increased safety and deterrence of violent or threatening behaviour, for example in Council's libraries or customer service centres.
- Potential negative impacts to vulnerable community members, for example to people without secure housing as they may have less privacy in public spaces.
- Potential for increased surveillance of groups that may have historically had negative experiences with government and/ or surveillance, for example culturally and linguistically diverse or indigenous Australians.

- Potential for use of technology such as facial recognition may impact more on some groups within society (noting such technology is not within the scope of this policy).

Crime Prevention through Environmental Design (CPTED) principles should be considered as a 'first line of defence' to improve safety, prior to installation of cameras. This may include measures such as better lighting or improving sight lines with an overall aim to improve safety, and perceptions of safety.

These impacts have been considered in the design of the policy. Following the Victorian Law Reform Council and VAGO principles will adequately address these potential negative impacts and ensure that the impacts of surveillance technology is positive.

A Gender Impact Assessment will be required for each application for surveillance technology, and assessed accordingly by the Surveillance Oversight Committee.

6. Supporting documents

This policy should be read in conjunction with all other relevant, Council policies and procedures, as well as relevant legislative requirements.

Related Legislation

- *Privacy and Data Protection Act 2014 (Vic)*
- *Surveillance Devices Act 1999 (Vic)*
- *Privacy Act 1988 (Cth)*
- *Local Government Act 2020 (Vic)*
- *Gender Equality Act 2020 (Vic)*

Related Guidelines, Operational Directives or Policies

- Information Privacy Policy
- Privacy Impact Assessment template

7. Definitions and abbreviations

Body worn camera	A portable camera usually attached to the clothing that is used to record video and audio. It may also have a GPS tracker and / or the ability to communicate via voice or be activated as a duress alarm.
CCTV	A device capable of capturing and recording either still or video footage. Includes video cameras with or without the ability for live viewing of images, and "trail cameras" or similar devices capable of recording still or video footage. Devices may be on permanently, for specific times, or activated by movement.
Council	Alpine Shire Council
CPTED	Crime Prevention through Environmental Design (CPTED) refers to a holistic, multi disciplinary approach to crime prevention based on principles of urban design and the management of built environments. CPTED strategies aim to reduce victimisation, deter offender decisions that precede criminal acts, and build a sense of

	community so that people's connection to place helps to reduce crime and improve perceptions of safety.
Personal Duress Alarm	A device used to monitor the location of an individual, and send an alarm to a remote location when activated to do so by the user. It may also be capable of recording audio and / or video. Similar to a Body Worn Camera except the primary purpose is user safety, rather than recording evidence.
Private conversation	A conversation that is carried out in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard only by themselves. It does not include a conversation made in circumstances where the parties to it ought reasonably to expect that it may be overheard by someone else.
Public place	Includes any area where the public has access as part of right or by invitation, whether expressed or implied, and whether a charge is made for admission. This includes public streets, malls, shopping centres, parks, publicly accessible buildings such as Council offices, libraries or recreation facilities, or other places where the public is present or permitted to have access.
Surveillance	Refers to the monitoring and analysis of data to collect information about individuals, groups or contexts. Surveillance is regulated by the <i>Surveillance Devices Act 1999</i> (Vic).
Surveillance Device	A device capable of capturing data, images or audio, that is used to conduct surveillance, or that may conduct surveillance regardless of whether it is intentional, or the primary purpose of the device.
Web camera	A camera used to live stream images or video to the internet. Typically, web cameras do not actively record (i.e. footage is not stored) and typically no audio is recorded.

8. Approval

THE COMMON SEAL OF THE
ALPINE SHIRE COUNCIL was
hereunto affixed this 30 day of June
2026
in the presence of:


COUNCILLOR


COUNCILLOR


CHIEF EXECUTIVE OFFICER

Version 1 of the Surveillance
Technology Policy was adopted
at the Ordinary Council Meeting
held on 30 June 2026.

The signed copy is held in
Council's records.