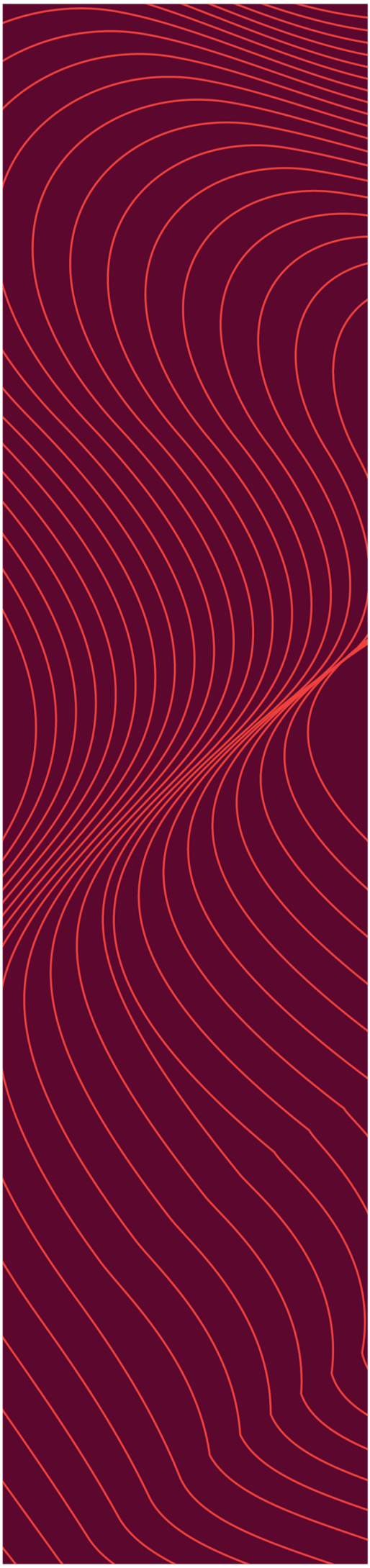
LATROBE CITY COUNCIL

Electronic Surveillance Policy

Version no 4

Approval date: 22 September 2025

Review date: September 2029



Document control

Responsible GM	Tim Ellis	
Division	Regional City Strategy and Transition	
Last updated (who and when)	Senior Compliance Officer	2025

Document history		
Authority	**Date**	**Description of change**
Council	07 Feb 2011	Adoption of Policy
Council	01 April 2019	Review and adoption of Policy
Council	02 August 2021	Review and adoption of Policy, including update of requirements for prior approved clubs and third-party systems, responsibilities, and associated forms and processes.
Council	22 September 2025	Review and update, including to reporting requirements, allowing approval of systems in exceptional circumstances not otherwise covered, transfer of some detail to the revised operational policy.
References	Refer to Section 8 and 9 of this Policy	
Next review date	August 2029	
Published on website	Yes	
Document reference no.	2238916	

1. Background

1.1. This Electronic Surveillance Policy (Policy) has been developed in the interests of contributing to public safety and/or the protection of Latrobe City Council (Council) staff and assets. The *Surveillance Devices Act 1999* and the *Privacy and Data Protection Act 2014* regulate the usage of electronic Surveillance Devices, including closed circuit television (CCTV), and how data collected through those devices is handled and stored.

2. Objectives

2.1. To provide the appropriate framework for the implementation, installation, data management and operation of electronic surveillance equipment by Council.

2.2. To ensure that Council's use of electronic surveillance is compliant with relevant legislation and aligned with community expectations.

2.3. To facilitate electronic surveillance capabilities that are sufficient and appropriate for protection of people and infrastructure/assets.

3. Scope

3.1 This Policy applies to all Council owned or operated surveillance systems excluding promotional/marketing footage captured for Council or at a Council event.

3.2 This Policy applies to all Council employees, contractors and volunteers.

3.3 This Policy does not apply to:

(a) temporary or non-fixed electronic surveillance systems used to capture traffic data or asset condition data, which is to be managed under a separate procedure; and

(b) occupiers of Council sites utilising their own CCTV system, except for section 4.3.4 which applies to all such systems.

4. Principles of management

4.1. Types of Surveillance Systems

4.1.1. Council's electronic surveillance systems and devices fall into two main types:

- Public Safety CCTV Systems; and
- Corporate Surveillance: includes but is not limited to permanent and temporary CCTV cameras/systems, body worn cameras, mobile duress alarms, and vehicle safety tracking devices on Council controlled vehicles.

4.2. Intent and Purpose

4.2.1. The intention of permanent and temporary placement and use of surveillance systems may be to:

- protect people and infrastructure through real time monitoring.
- enhance public safety through deterring unwanted behaviour and provide support in emergencies or active threat situations.
- facilitate effective management of Council services and facilities.

- assist in the investigation of and response to crimes against Council assets or personnel or other serious incidents.

4.3. Approval of Surveillance Systems/Devices

4.3.1. The Chief Executive Officer (CEO) is authorised to approve, disapprove or revoke the use/implementation of surveillance systems/devices.

4.3.2. The following parameters apply when considering what will be approved:

- the proposed surveillance is for a legitimate Council objective or function and consistent with applicable laws;
- the intended purpose is consistent with this Policy;
- alternatives to surveillance have been considered;
- for Public Safety CCTV Systems, consultation has occurred with affected communities, key stakeholders and Law Enforcement Agencies, including but not limited to, Victoria Police which would have direct access to the system pursuant to section 4.6.1 of this Policy;
- for Corporate CCTV Systems, consultation has occurred with affected stakeholders (e.g. staff, patrons, clubs at recreation reserves etc.);
- the impacts on privacy and whether the proposed surveillance is a fair response to the issue or risk being addressed, including whether visual and/or audio capability is appropriate;
- how the surveillance information and data will be kept secure and protected from inappropriate use or disclosure;
- costs (for the establishment, operational and replacement costs i.e. whole of life-cycle costs for an average ten-year cycle) and benefits; and
- how the effectiveness of the surveillance activity will be measured.

4.3.3. The following will not be approved:

- the use or placement of dummy cameras;
- the use of drones for surveillance activities;
- the placement of Surveillance Devices within toilets, washrooms, change rooms or the like;
- audio capability on Corporate CCTV Systems unless there are exceptional circumstances, i.e. where it provides high impact in terms of personal safety or asset protection, and an assessment of privacy impact supports its use; or
- any device that does not meet the requirements of this Policy, unless in exceptional circumstances with CEO approval.

4.3.4 Occupiers of Council sites under lease or licence that are operating their own CCTV system must enter a written agreement with Council, which will include a requirement to comply with the Information Privacy Principles under the *Privacy and Data Protection Act 2014* and relevant legislation. The agreement will also include maintaining an access/extraction/disclosure register, signage, and completing appropriate training prior to use. Management of these systems may be subject to periodic review by Council officers, and if they do not comply, Council may remove the users' system.

4.4. Signage

4.4.1. Where electronic surveillance is occurring, appropriate notification will be provided to indicate that the area or activity is being observed or recorded.

4.4.2. For fixed location surveillance (such as CCTV and dashcam), signage will be installed and maintained to comply with relevant Australian Standards in force from time to time and must comply with the following requirements:

- Signs will be placed at each main point of access to the surveillance coverage area.
- Organisational guidelines on sign content, layout and any other requirements must be followed. Signs will be prepared so as to be easily understood by members of the public, including people who are from non-English speaking backgrounds. This should include by use of a mix of worded text and symbols.
- Where CCTV with audio capability is operating, this must be clearly indicated on the signage within that area.
- Signs will be clearly visible, distinctive and located in areas with good lighting, placed within normal eye range and large enough so that any text can be read easily. Footpath marking with the camera symbol only may also be used in public areas.
- Signs will identify the organisation/owner of the system undertaking surveillance.
- Signs will direct persons with queries about the system to contact Council using the 1300 367 700 number.
- Signs will be checked regularly for damage and theft, and replaced where required.

4.4.3. The location or placement of any non-fixed Surveillance Devices will not be required to have signage. Notification will be provided via other suitable means, such as a verbal statement by Council officer where possible to do so (e.g. safety risks might mean it is not possible to provide such notification) and through information available within this Policy and otherwise available on Council's website.

4.4.4. Where electronic surveillance is no longer occurring, all signage and equipment must be removed as soon as practicable.

4.5. Data Security

4.5.1. Data collected, in accordance with the intention of this Policy, is not collected for the purpose of public access to the data.

4.5.2. For Corporate CCTV systems, the surveillance data on digital media will be retained for 31 days unless otherwise downloaded for permitted administrative use, legal reasons or as required by a Law Enforcement Agency.

4.5.3. Unless otherwise required by a Law Enforcement Agency or by law, all surveillance camera footage is temporary and will be destroyed when the relevant administrative use has concluded.

4.5.4. Data collected by any surveillance system for the purposes of enforcement shall be stored securely in a centralised location. Any evidence obtained and retained for the purposes of enforcement shall be collected, managed and stored in accordance with the *Evidence Act 2008*.

4.5.5. Council will ensure that its record keeping practices comply with the Public Records Office Standards for the management of public records, Public Records Office Specifications and the *Public Records Act 1973*.

4.5.6. Where footage has been provided to a Law Enforcement Agency, it will be the Law Enforcement Agency's responsibility to retain the records/footage in accordance with the disposal authority that covers that Law Enforcement Agency's functional responsibilities.

4.5.7. Where footage is to be provided to a third party that is not a Law Enforcement Agency outside of a legislative process such as freedom of information or subpoena, Council will specify any terms on which the footage is being provided.

4.6. Direct Access to Public Safety CCTV Systems by Law Enforcement Agencies

4.6.1. Where the CEO has approved the installation of a Public Safety CCTV System, Victoria Police will be given direct access to it. However a written agreement for management of that access must be in place prior to implementation of the system.

4.6.2. The agreement will cover:

- obligations and responsibilities of Council and Victoria Police;
- ownership of the surveillance system and the data it generates; and
- oversight and review mechanisms, including how Council will be assured that Victoria Police is using and managing the information provided appropriately.

4.6.3. No agreement will be entered into with any other Law Enforcement Agency for direct access to a Public Safety CCTV System unless approved by the CEO in exceptional circumstances.

4.7. Access to Data

4.7.1. Access to and use and disclosure of captured data from a surveillance system shall be in accordance with the *Privacy and Data Protection Act 2014*.

4.7.2. Access will generally be in the form of retrospective review after an incident; however, in relation to Corporate CCTV Systems passive monitoring will be undertaken as considered necessary taking into account the purpose of the particular System.

4.7.3. Access to Corporate Surveillance System data collected shall be restricted to authorised users, being the following:

- CEO;
- Public Interest Disclosure Coordinator and Officers;
- Privacy Officer;
- Freedom of Information Officer;
- A member of Council staff authorised as per the relevant operational policy or procedure;
- a Contractor, but only in the absence of a member of Council staff being qualified or available to access the data and only to the extent specified and authorised by the Manager Governance; and
- any external person conducting an internal investigation or audit, as approved by the Manager Governance, involving suspected unlawful activity or claim against Council.

4.7.4. A Corporate CCTV System Access, Extraction and Disclosure register will be maintained, with each access registered as to why data was accessed and by whom. The register will

be regularly reviewed by authorised users and Governance, as per responsibilities under section 5.

4.7.5. Access must not be through a generic or shared user login.

4.7.6. Equipment used to capture and store surveillance data will be stored in a way that to the extent practicable, prevents the risk of unauthorised access, tampering or data theft.

4.7.7. Any request for access to data by a third party, other than a Law Enforcement Agency, is to be made through Council's Freedom of Information process or via other CEO approved internal processes as appropriate.

4.8. Related Operational Policies and Procedures

4.8.1. An operational policy will be in place for Corporate CCTV Systems together with a procedure for each other type of Surveillance Device, which will be consistent with the requirements of this Policy. These documents will be provided to system users and reviewed periodically.

4.8.2. Council's Information Technology (IT) Department will provide site and system specific training and information to authorised users.

4.9. Inappropriate Use and Complaint Handling

4.9.1. Council officers who work with surveillance systems are to comply with the requirements of this Policy.

4.9.2. Where a Council officer is in breach of this Policy, there will be an internal review and appropriate action will be taken in accordance with the Staff Code of Conduct.

4.9.3. Any public complaints or requests in relation to any aspect of a surveillance system relating to Council should be made in writing to:

Latrobe City Council

PO Box 264

Morwell VIC 3840

Or by email at: latrobe@latrobe.vic.gov.au

4.9.4. All complaints will be handled in line with the *Complaints Handling Policy*, available on Council's website.

4.9.5. Any member of the public that is dissatisfied with the outcome of their complaint to Council also has the right to complain to the Victorian Ombudsman using the following contact details:

Victorian Ombudsman

Level 2/570 Bourke Street, Melbourne Victoria 3000

Email: ombudvic@ombudsman.vic.gov.au

Phone: 1800 806 314

Website: https://www.ombudsman.vic.gov.au

A complaint in relation to a breach of the Information Privacy Principles can be made to the Office of the Victorian Information Commissioner using the following contact details:

Office of the Victorian Information Commissioner

PO Box 24274, Melbourne VIC 3001

Email: enquiries@ovic.vic.gov.au

Phone: 1300 006 842

Website: https://ovic.vic.gov.au

5. Accountability and responsibility

Accountability and responsibility for this Policy is outlined below.

5.1 Council

- Responsibility to ensure this Policy is consistent with Council's Strategic Direction and other 'Council policies.
- Responsibility for the decision to approve this Policy by Council Resolution.

5.2 Chief Executive Officer

- Overall responsibility for:
  - compliance with this Policy;
  - enforcing accountability;
  - providing resources; and
  - performance monitoring.
- Approves the use of Electronic Surveillance Devices.
- Approves the outsourcing of Electronic Surveillance Devices.

5.3 General Manager

- Responsibility for:
  - compliance with this Policy;
  - enforcing accountability;
  - providing resources; and
  - performance monitoring.

5.4 Governance

- Responsibility to ensure this Policy is reviewed in accordance with the requirements as set.
- Recommends the inclusion of an audit on Electronic Surveillance in the ongoing *Internal Audit Plan*.
- Develops and maintains the Corporate CCTV System Operational Policy.
- Ensures training and support is provided to staff prior to access to Corporate CCTV Systems being authorised.
- Manages the Corporate CCTV register.
- Prepares and provides reporting, evaluation and audit of Corporate CCTV Systems and system management.
- Manager Governance authorises access to Corporate Surveillance System data, including members of staff, contractors and internal investigators/ auditors.

5.4 Information Technology Services

- Evaluates all requests for surveillance equipment compliance in accordance with the *IT Security Framework.*
- Manages security, maintenance, upgrade and repair of Corporate CCTV Systems, Surveillance Devices and data.
- Provides a central register of Corporate CCTV System data extracted in accordance with this Policy and with the *Records Management Policy*.
- Provides and maintains Corporate CCTV System access and training for authorised users.

5.4 Authorised Users

- Adherence to this Policy and the relevant Operational Policy and/or procedure.
- Compliance with relevant legislation.
- Monitoring of systems in accordance with the relevant Operational Policy and/or procedure.
- Use of Corporate CCTV System Access, Extraction and Disclosure register.
- Contribute to regular review and reporting, and periodic evaluation, of Electronic Surveillance systems within their remit.
- Regular inspection of Corporate Surveillance Systems/Surveillance Devices for damage, theft and proper operation.

5.5 Users of approved non-Council CCTV Systems

- Compliance with section 4.3.4 of this Policy and the agreement entered into pursuant to that section.

5.6 Employees, Contractors and Volunteers

- Participate where required in the development of frameworks and procedures in compliance with this policy.
- Comply with frameworks and procedures developed to achieve compliance with this policy.

6. Evaluation and Review

6.1. Evaluation

6.1.1. Ongoing evaluation and regular reporting of the surveillance system against the objectives and purpose of the system, and against documented performance standards annually.

6.1.2. Public Safety CCTV Systems will be evaluated in accordance with the written agreement in place with Victoria Police.

6.1.3. Corporate Surveillance Systems will undergo periodic audits with appropriate action plans to be formulated to address any deficiencies. Audits may include independent audits, and self-audits.

6.2. General Reporting

6.2.1. Public Safety CCTV Systems will be reported on in accordance with the written agreement in place with Victoria Police.

6.2.2. A report will be provided to the General Manager Regional City Strategy and Transition quarterly to assist in the identification of any suspicious or inappropriate use of Corporate Surveillance Systems/Devices. This report will contain:

- the number of incidents requiring review of surveillance data;
- how many times footage has been downloaded or copied and the reasons for this action (obtained from Access, Extraction and Disclosure Register and system activity logs where available);
- the number of requests for footage;
- the number of complaints;
- how many times footage has been released, to whom, for what reason, and who authorised the release; and
- a summary of maintenance issues.

6.3. Review Cycle

6.3.1. It is recognised that, from time to time, circumstances may change leading to the need for minor administrative alterations to this Policy. Where an update does not materially alter this Policy, such a change may be made administratively. Examples include updating to the latest style/template for policies, a change to the name of a Council department or applicable responsible position, a change to the name of a Federal or State Government department, and a minor update to legislation which does not have a material impact.

6.3.2. Any change or update which materially alters this Policy must be by resolution of Council.

6.3.3. This Policy will be reviewed and updated at least once every four years, unless one of the following occurs first:

- significant changes to legislation applicable to this Policy; or
- upon request of Council.

7. Definitions

In this Policy

Authorised User	Council officers and other individuals listed at paragraph 4.7.3.
Body Worn Cameras	A wearable audio, video or photographic Surveillance Device.
Corporate Surveillance System	Where one or more Surveillance Devices are used to monitor facilities that include Public Places such as Council offices, pools, libraries, performing arts centres and waste management facilities and includes Body Worn Cameras, mobile duress alarms and vehicle tracking devices.
Corporate CCTV System	Council owned or managed closed-circuit television system operating in and around Council facilities.
Complaint	An expression of dissatisfaction with a specific action or service of a public body, including the failure by a public body to comply with its public service charter or mission.

Complaint handling process	The way individual complaints are dealt with by a public body including the policy, procedures, practices and technology.
Council	Latrobe City Council.
Disclosure	Access to and disclosure of surveillance data to third parties (including unauthorised Council officers).
Law Enforcement Agency	Means any agency (including a regulatory agency) that is charged under applicable law with the enforcement of legislation of the State of Victoria or the Commonwealth of Australia.
Passive monitoring	Where surveillance monitors are intermittently viewed by operators.
Public Place	In accordance with the *Summary Offences Act 1966*, a public place includes: • any public highway, road, street, bridge, footway, footpath, court, alley, passage or thoroughfare even if it is on private property • any park, garden reserve or other place of public recreation or resort • any railway station, platform or carriage • any public vehicle available for hire • any government school • any market. For the purposes of this Policy, this definition also includes places owned, managed or controlled by Latrobe City Council to which the public are permitted to have access, such as Council offices and other buildings and locations, including sport, leisure and recreation facilities.
Public Safety CCTV System	Where one or more Surveillance Devices are used to discourage and detect antisocial and criminal behaviour in Public Places. Victoria Police can have direct access to monitor and review footage from these systems.
Surveillance Device	In accordance with the *Surveillance Devices Act 1999*, surveillance devices include the following: • Data Surveillance Devices • Listening Devices • Optical Surveillance Devices (visually records or observes an activity) • Tracking Devices (including vehicle tracking and mobile man-down alarms) • Body Worn Cameras

8. Related Documents

- *Privacy Policy*
- *IT Security Framework*
- *Records Management Policy*
- *Corporate CCTV Systems Operational Policy*
- *Body Worn Video Camera Procedure*
- *Mobile Duress Alarm Procedure*

9. Reference Documents

- *Security and Privacy of Surveillance Technologies in Public Places – Victorian Auditor–General's Office - September 2018*
- *Closed Circuit Television in Public Places – Guidelines - Victorian Ombudsman – November 2012*
- *Guidelines to surveillance and privacy in the Victorian public sector – Commissioner for Privacy and Data Protection – May 2017*
- *Guide to developing CCTV for Public Safety in Victoria – Department of Justice and Regulation – June 2018*
- *Surveillance Devices Act 1999*
- *Summary Offences Act 1966*
- *Evidence Act 2008*
- *Privacy and Data Protection Act 2014*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Freedom of Information Act 1982*