

HOBSONS
BAY CITY
COUNCIL



CCTV Policy

Acknowledgment of Country

Council acknowledges the Bunurong People of the Kulin Nation as the Traditional Owners of these municipal lands and waterways, and pay our respects to Elders past, present and emerging.

Contents

1. Introduction.....	4
1.1. Purpose.....	4
1.2. Scope.....	4
2. Policy Context.....	4
3. Definitions	5
4. Policy Statement.....	5
5. Policy Development.....	6
5.1. Applicable Legislation and Polices	6
6. Governance and Responsibilities	6
7. Mandatory Criteria for Installation	7
7.1. Investment	7
8. CCTV Operation	7
8.1. Authorised Officers	7
8.2. Privacy and Data Protection.....	8
8.3. Training.....	8
8.4. Artificial Intelligence	8
9. Audit and Review.....	8
10.Complaints and Enquiries.....	9
11.References / Related Documents	9
12.Monitoring, Compliance, Reporting and Review	9
13.Document Control and Version History.....	9

1. Introduction

1.1. Purpose

This policy sets out Hobsons Bay City Council's approach to the installation, use, and management of Closed-Circuit Television (CCTV) and other visual surveillance devices within Council-owned or controlled facilities and for the purposes of illegal dumping monitoring and prevention.

It ensures that all surveillance activities:

- Are used for legitimate purposes such as staff, contractor, and visitor safety, asset protection and facility security,
- Are used for the purpose of monitoring and prevention of illegal dumping of waste within road reserves and public spaces
- Are managed in accordance with applicable legislation, privacy principles, and Council's ethical and governance standards.
- Do not extend to general monitoring of public spaces or the wider community environment.

1.2. Scope

This policy applies to all fixed or mobile CCTV and visual surveillance systems that:

- Are owned, leased, or operated by Council, and
- Are installed within or immediately adjacent to Council facilities, buildings, depots, and operational assets for security and safety purposes.
- CCTV used in road reserves and public spaces for the purposes prevention and monitoring of illegal dumping of waste

This policy does not apply to:

- Public-space CCTV networks or community-safety camera programs operated by external agencies (e.g., Victoria Police or traders' associations).
- Use of personal devices or cameras by staff for incidental recording.
- Temporary event-specific cameras, which require separate approval under the Event Management or Risk Management Framework.
- CCTV used for the purpose of general monitoring of road reserves and public spaces
- Dashboard cameras used on fleet vehicles.

2. Policy Context

Council is responsible for providing safe, accessible and well-managed public spaces for the community. In some locations, persistent safety risks, antisocial behaviour, property damage and public safety incidents place pressure on Council to adopt measures that support prevention, monitoring and response.

CCTV systems are one tool that may assist in deterring criminal behaviour, supporting investigations, and improving incident response when used appropriately. However, CCTV also

raises important considerations relating to privacy, data protection, proportionality, transparency and community trust.

Legislative requirements relating to privacy, surveillance devices, public records and information security place obligations on Council regarding the collection, use, storage and disclosure of CCTV footage. Inconsistent or ad-hoc use of CCTV can expose Council to legal, financial and reputational risk.

A clear policy is required to define the circumstances in which CCTV may be installed and operated in public places, ensure compliance with legislative and ethical requirements, and balance public safety objectives with individual privacy rights.

3. Definitions

For the purposes of this policy:

CCTV	Closed-Circuit Television
HBCC	Hobsons bay City Council
CPTED	Crime Prevention Through Environmental Design
AI	Artificial Intelligence

4. Policy Statement

Hobsons Bay City Council supports the responsible and proportionate use of CCTV and surveillance devices to:

- Protect staff, contractors, and visitors from harm.
- Safeguard Council buildings, plant, vehicles, equipment, and materials.
- Deter and investigate damage, theft, vandalism, or unauthorised access.
- Support emergency response and incident review processes.
- Prevent and monitoring of illegal dumping of waste

Council will not use CCTV or surveillance devices to monitor employee performance or general work activity.

Council will ensure that:

- Every camera installation is supported by a clear documented purpose and risk-based justification.
- Devices are installed and operated in compliance with relevant legislation and privacy obligations.
- Recorded information is securely stored, retained only as long as necessary, and accessed only by authorised personnel.
- Requests for access to footage are managed through defined, auditable processes.
- Signage is displayed wherever CCTV is in operation, informing individuals that they may be recorded.

5. Policy Development

5.1. Applicable Legislation and Policies

This policy operates under and must comply with:

- Surveillance Devices Act 1999 (Vic)
- Privacy and Data Protection Act 2014 (Vic)
- Public Records Act 1973 (Vic)
- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Freedom of Information Act 1982 (Vic)
- Relevant Australian Standards for electronic security systems
- Council's Information Privacy Policy and Records Management Policy
- Councils' Artificial Intelligence (AI) Policy

6. Governance and Responsibilities

Role	Responsibility
CEO / Executive Leadership Team	Approve this policy and significant CCTV installations; ensure resources and compliance.
Director Infrastructure & City Services	Strategic oversight of CCTV operations within the organisation.
Manager City Operations	Custodian of this policy; maintains the master register of CCTV devices; ensures maintenance, signage, and staff training.
IT and Information Security	Manage digital storage, data protection, and secure network connections.
Coordinator Governance	Provide privacy impact assessments, compliance advice, and respond to FOI or data-access requests.
Facility Maintenance Unit	Identify facility risks; request CCTV installations; ensure local staff understand use and limitations.
All Employees and Contractors	Comply with this policy and report any misuse or breach.

7. Mandatory Criteria for Installation

Each new CCTV installation must be supported by a Risk Assessment and Business Case that demonstrates:

- 1) One of the below:
 - a) A documented safety or security issue at the facility (e.g., repeated vandalism, theft, unauthorised entry, or staff safety concern).
 - Or a
 - b) A documented incident of illegal dumping of waste
- 2) That CPTED (Crime Prevention Through Environmental Design) or non-surveillance measures (lighting, access control, alarms) have been considered.
- 3) That the proposed camera location, field of view, and recording parameters are proportionate to the purpose and do not unnecessarily capture public areas.
- 4) That funding for installation, maintenance, and data storage has been identified in the Facilities Renewal or IT Budget.
- 5) Approval has been granted by the Director Infrastructure & City Services following review by the Manager City Operations.

7.1. Investment

Council's future investment into CCTV will be informed by:

- Priorities identified in the Council Plan
- Available funding in Council's annual budget.

8. CCTV Operation

- CCTV systems will normally record only. Live feeds are accessible by approved staff only. CCTV system and alarms work intermittently of each other
- Recorded footage will be retained for 31 days, unless required for an incident investigation or legal proceeding.
- Access to live or recorded footage is limited to authorised officers for security, safety, or legal purposes.
- The security contractor responsible for providing the CCTV camera installation and software will have access to specific time periods only when requested by an approved officer for an applicable purposed under this policy
- Requests for access from external parties (e.g., Victoria Police, insurers, external legal representatives) must be made in writing and receive dual approval from Manager City Operations and Director Infrastructure and City Services, with a record kept of each release.
- Requests for access made under Freedom of Information are to comply with and be assessed under the Freedom Of Information policy
- Data will be stored in secure Council servers or approved cloud storage with encryption and access logs.

8.1. Authorised Officers

The below roles are authorised officers under this policy

Approval Officers

- Chief Executive Officer
- Director Infrastructure and City Services

Operational Access

- Manager City Operations
- Coordinator Facilities

Oversight and IT Access

- Director Corporate Services
- Manager Corporate Integrity
- Manager Digital Services
- Chief People Officer

For the purposes of implementing this policy the authorised officers may delegate responsibility. Authorised officers may only access footage where reasonably necessary and proportionate to their role. Delegation must be done in writing stipulating the parameters under delegation is provided.

8.2. Privacy and Data Protection

Council acknowledges that CCTV involves collection of personal information under the *Privacy and Data Protection Act 2014 (Vic)*.

Council will:

- Collect only information necessary for its stated security purposes.
- Limit viewing and disclosure to authorised persons.
- Securely destroy or overwrite recordings after the retention period.
- Display signage at each entry point where cameras operate, providing contact details for enquiries.
- Maintain a CCTV Register listing each device's location, purpose, responsible officer, and retention period.

8.3. Training

All staff who operate, review, or maintain CCTV equipment must complete induction training covering:

- Purpose and limitations of Council CCTV;
- Privacy obligations;
- Procedure for access and disclosure;
- Reporting of faults or suspected misuse.

8.4. Artificial Intelligence

All use of Artificial Intelligence will comply with Council's AI policy

9. Audit and Review

- The Coordinator Facility Services will conduct an annual audit of all CCTV devices to confirm operation, signage, data security, and compliance.
- Findings from this audit will be reported to the Executive Leadership Team.

- This policy will be reviewed every three years, or sooner if required by legislative or technological change.
- Any device or material found to be non-compliant will result in decommissioning of the device.

10. Complaints and Enquiries

Any person who believes their privacy has been compromised by Council's CCTV operation may lodge a complaint in writing to Council's Privacy Officer. If unresolved, they may refer the matter to the Office of the Victorian Information Commissioner (OVIC).

11. References / Related Documents

- Office of the Victorian Information Commissioner – Guiding Principles for Surveillance in the Public Sector (2021)
- Glen Eira City Council CCTV Policy (2020)
- Knox City Council Visual Surveillance Devices Policy (2019)
- Banyule City Council Surveillance in Public Places Policy (2022)
- Merri-bek City Council CCTV Surveillance Policy (2021)
- Boroondara City Council Code of Practice for Security Camera Management (2022)
- Darebin City Council Surveillance Systems Policy (2020)

12. Monitoring, Compliance, Reporting and Review

1. The digital services team will support facilities with the implementation of this policy by providing training to authorised officers
2. The Corporate Integrity team will be notified receive reports about the application of this policy.
3. This policy will be reviewed by the City Operations team or in response to legislative changes, council direction or operational needs.

13. Document Control and Version History

Policy Name:	CCTV Policy
Responsible Directorate	Infrastructure and City Services
Policy Owner	Manager City Operations
Policy Type	Council Policy
Date Adopted by	July 2026
Review Date	July 2030

Version Number	Date	Approved by
0001	28 th July 2026	Council