Central Coast Council

Closed Circuit Television Policy

Date Adopted: **XX/XX/20XX**
Revision: **X**

Table of Contents

1. Policy Objectives

1.1. The Closed Circuit Television (CCTV) Policy (Policy) is part of an integrated community safety strategy aimed at reducing the potential for crime and anti-social behaviour in the Central Coast Local Government Area (LGA) by achievement of the following objectives:

1.1.1. To reduce the level and fear of crime by deterring potential offenders.

1.1.2. To assist Police and other regulatory agencies in determining the appropriate allocation of resources.

1.1.3. To assist Police and other regulatory agencies in the detection and prosecution of offenders.

1.1.4. To enhance perceptions of safety for all people who live in, work in and visit the Central Coast as part of an integrated community safety strategy.

1.1.5. To support environmental and coastal monitoring initiatives.

1.1.6. To support operational requirements.

---

2. Policy Scope

2.1. This Policy applies to all Council representatives and, where relevant, members of the public.

2.2. Subject to the exclusions set out in clause 2.3 below, this Policy applies to the Council-owned CCTV Systems installed, operated, or managed by or on behalf of Council at locations in the Central Coast Local Government Area (LGA) including Council buildings, facilities, and public places (including major or special events and traffic management) that has the purpose of effective management of Council facilities and operational efficiencies, environmental monitoring, surveillance or supporting enforcement activities by the NSW Police Force and Authorised Officers of Council. This includes:

2.2.1. cameras in or on Council property.

2.2.2. cameras for the purposes of coastal and beach monitoring.

2.2.3. mobile surveillance and fixed cameras for the purpose of community safety, risk management and crime prevention.

2.2.4. cameras used for environmental monitoring.

2.3. This Policy does not apply to:

2.3.1. any CCTV installed by a community-based organisation who lease Council facilities or installed by or on behalf of another Government agency. These requests will need approval from Council prior to installation. Council staff will consider how the proposed request aligns with the principles of this Policy prior to approving requests for CCTV

installation. If approved, the CCTV will be owned and operated by the organisation in accordance with appropriate legislation and guidelines.

2.3.2. Cameras attached to garbage trucks under Council's contracts for garbage collection.

2.3.3. Time-lapse cameras for the purpose of construction monitoring.

2.3.4. Any CCTV installed by or on behalf of the lessee, licensee or third-party manager of a Council-controlled property or premises. Subject to any provisions in a lease, licence or management agreement to the contrary, consultation is required prior to the installation or operation of CCTV on leased, licensed and externally managed property premises. Council will not unreasonably refuse or restrict the installation or operation of CCTV in such circumstances. If approved, the CCTV will be operated by the relevant party in accordance with appropriate legislation and guidelines.

2.3.5. Any CCTV installations which may be required under superseded or future legislation.

3. Policy Statement

3.1. Principles of CCTV

3.1.1. The following principles shall guide the use of CCTV within Council, and no one principle should be applied to the detriment of another. Principles must be collectively considered and applied to the extent that is reasonable and practicable in the circumstances.

3.2. Ethical and Responsible Use of CCTV

3.2.1. All CCTV owned and managed by Council in the LGA will be operated ethically and responsibly, within the bounds of all applicable legislation, and only for the purposes for which it has been established or which are subsequently agreed to in accordance with this Policy.

3.3. Public Interest

3.3.1. All CCTV operations will be conducted with due regard to the privacy and civil liberties of individual members of the public.

3.4. Accountability

3.4.1. Council will be accountable to the public for ensuring the security, integrity, and effectiveness of all CCTV installations that are covered by this Policy. Accountability will be maintained through regular monitoring and evaluation of CCTV operations.

3.5. Partners

3.5.1. All contact related to CCTV operations between Council, security control operators, contractors, the NSW Police Force and any approved stakeholders will consider Council's Code of Conduct and parameters established in this Policy.

3.6. Recording of Material

3.6.1. In relation to CCTV installations that are covered by this Policy, material will only be recorded and retained for the purposes provided in this Policy and in accordance with the privacy conditions outlined in all applicable privacy legislation.

3.7. Internal Access to CCTV Footage

3.7.1. Access to the information recorded on CCTV systems will be restricted to those employees who have been trained to operate the system and/or to contractors engaged by Council to maintain and monitor any surveillance system.

3.7.2. Certain employees and/or contractors may be granted access to live CCTV footage where there is a demonstrated operational need. This access is strictly limited to roles where real-time monitoring is essential for safety, security, or operational efficiency. Employees with such access must adhere to this Policy. Access provisions will be reviewed regularly and may be revoked if no longer required or if a breach of this Policy occurs.

3.7.3. Council employees may request access to CCTV footage, noting:

a) Where a request to access CCTV footage is made by any employee such access shall require authorisation by either the Disclosures and Investigations Coordinator, Unit Manager People and Culture or the Chief Executive Officer subject to the consideration of the applicable laws.

b) Requests for access to CCTV footage will include a reason for access and an expiry date that access will be cancelled.

c) Council employees shall at all times exercise a duty of confidentiality. Data shall only be released in compliance with the *Workplace Surveillance Act 2005* and as prescribed by this Policy.

3.7.4. Councillors are not authorised to access live or recorded CCTV footage. Any requests for CCTV related information must be managed in accordance with this Policy and applicable legislation.

4. Responsibilities

4.1. CCTV Monitoring and Management

4.1.1. Council is responsible for maintenance, management and security of all Council owned and managed CCTV and for ensuring compliance with this Policy.

4.1.2. In specific circumstances, Council may formally transfer responsibility for CCTV systems to another party. Such delegation must be documented in writing.

4.2. Responsible Officer

4.2.1. The Unit Manager, Projects and Asset Management is the Responsible Officer for this Policy and is responsible for keeping this Policy current.

4.2.2. The Unit Manager, Projects and Asset Management is responsible for determining what constitutes access for operational purposes and activities classed as operational purposes.

4.2.3. The Unit Manager, Projects and Asset Management, or approved delegate, is responsible for reviewing and authorising NSW Police or other Government Agency requests for access to CCTV footage.

4.3. Chief Executive Officer

4.3.1. Council has delegated the Chief Executive Officer the authority to exercise the responsibilities detailed in this Policy.

4.4. Directors

4.4.1. Directors are responsible for ensuring their Directorate adheres to the requirements of this Policy.

4.5. Employees

4.5.1. Employees, Councillors and contractors must adhere to the requirements of this Policy and operate within its authorities.

5. Public Interest

5.1. Where CCTV is in operation, signs advising that CCTV is in operation will be displayed in the area. These signs will:

5.1.1. Allow members of the public entering the area to make a reasonable approximation of the area covered by the CCTV.

5.1.2. Identify Council as the owner of the CCTV and provide contact details should further information be required.

5.1.3. Adhere to legislative requirements.

5.2. Use of all CCTV will be consistent with the aims and objectives articulated within this Policy.

5.3. Use of CCTV to observe a private and/or commercial premise is prohibited and all reasonable efforts will be employed to limit such access through camera programming and placement.

5.4. Camera placement will be determined in alignment with Council's objectives, ensuring strategic positioning to effectively capture the desired field of view while maintaining visibility to the public

5.5. "Dummy" cameras will not be used.

5.6. This Policy is available to the public on Council's website.

6. Accountability

6.1. Site Evaluation

6.1.1. Prior to the installation of any CCTV at a designated location, Council will undertake a preliminary evaluation of the level of risk in the area to establish a baseline against which CCTV operations can be evaluated. This evaluation includes a range of criteria, including but not limited to:

a) Crime statistics.

b) Local police reports and advice.

c) Safety of Council staff.

d) Public safety.

e) Coastal risk assessment concerns.

f) Internal risk assessment and recommendations of that assessment.

g) Evidence from standalone rapid deployment cameras to ascertain the level and nature of the criminal activity or anti-social behaviour (these cameras would be installed in compliance with this Policy).

h) Feasibility and cost of installing CCTV within current operating expenditure.

i) Operational need.

7. CCTV Operations

7.1. Council will be responsible for:

7.1.1. The day-to-day management of CCTV operations.

7.1.2. The installation, maintenance and replacement of all CCTV and related equipment in accordance with budgetary requirements.

7.1.3. The provision of training to all Council staff involved in the operation of CCTV and related equipment.

7.1.4. The monitoring, review, auditing and evaluation processes.

7.1.5. Consulting members of the public and other agencies in relation to CCTV operations and any proposed changes.

7.2. Installation and placement of CCTV cameras or other aspects of the CCTV system on Council property or in public places for which Council has operational responsibility (eg public roads, public reserves, waste and leisure facilities) will be solely at the discretion of Council in consultation with relevant stakeholders as appropriate.

8. Operational Needs

8.1. CCTV systems may be accessed and used to support Council's operational requirements beyond crime prevention and public safety. These include, but are not limited to:

8.1.1. Live Monitoring: Viewing live CCTV footage to support real-time operational decision-making, including incident response, safety, and environmental monitoring.

8.1.2. Recorded Footage Review: Accessing and reviewing recorded footage for operations including, but not limited to:

a) Environmental Monitoring: Observing environmental conditions, illegal dumping, wildlife activity, and other ecological concerns.

b) Post-Event Evaluation: Assessing incidents or events after they occur to improve future planning, safety protocols, and service delivery.

c) Dispute Resolution: Investigating complaints, service disputes, or community concerns where visual evidence may assist in clarifying facts.

d) Contractor Performance: Evaluating the conduct and performance of contractors and service providers in relation to agreed standards and obligations, together with Council's Workplace Surveillance Policy.

e) Number Plate Verification: Verifying vehicle entry/exit times. Where disclosure of footage is required, supporting information must be given to the Unit Manager, Projects and Asset Management or delegate to obtain written approval. When disclosing footage, you must use masking techniques for number plates or identifiable features of uninvolved parties to protect privacy.

8.1.3. Extended Retention Periods: Where footage is required for operational investigations, legal proceedings, or compliance audits, it may be retained for longer than the minimum 31-day period.

8.1.4. Restricted Disclosure: CCTV footage accessed for operational purposes shall not be disclosed, distributed, or provided to external parties unless required by law, subpoena, or formal legal process. Internal access must be limited to authorised personnel and logged for audit and accountability. Where disclosure of footage is required, supporting information must be given to the Unit Manager, Projects and Asset Management or delegate to obtain written approval.

9. Partners

9.1. NSW Police have access to view live footage of certain cameras within the LGA.

9.2. NSW Police will not be permitted to remove any recorded material, operate recording equipment, or have contact with any recorded material at any time unless under the terms of this Policy, submitting a formal application or subject to the execution of a search warrant or for other relevant legal purposes.

9.3. Any amendment in existing arrangements for NSW Police contact with and use of the system would amount to a significant change in CCTV operations and must be agreed to in accordance with the relevant provisions of this Policy before being implemented.

9.4. Any formal requests for CCTV footage or operational information by NSW Police will be recorded by Council staff and will be subject to audit.

9.5. The NSW Police Force will be required to supply a Letter of Compliance to Council advising the organisation of their adherence to this Policy on an annual basis.

10. Probity

10.1. Council will ensure consideration of the following items relating to probity:

10.1.1. All staff and contractors employed to work with the CCTV systems and equipment will meet the appropriate standards of probity and be given appropriate levels of training. The control of the system and all its contents will be protected from unauthorised access.

10.1.2. Systems of recruitment and selection of staff which include measures to ensure that the selection process provides for thorough validation of the suitability of candidates and regular review of the suitability of employed staff to work with CCTV systems and equipment.

10.1.3. A requirement that all staff are qualified at a suitable level on appointment and are capable of meeting in-service training requirements for the operation of CCTV systems and equipment.

10.1.4. Monitoring procedures to ensure staff are complying with any licensing or other requirements for the performance of their duties.

10.1.5. A disciplinary procedure to be employed if staff are found to have breached any of the provisions of this Policy or Council's Code of Conduct.

10.1.6. A requirement of confidentiality which can be enforced during and after termination of employment.

10.1.7. Systems of monitoring and supervision that ensure compliance with this Policy.

10.1.8. Only trained monitoring staff will have access to the CCTV operating systems, except in select cases where NSW Police may be granted emergency access to obtain footage, subject to approval by the Unit Manager Projects and Asset Management.

10.1.9. Operators of all CCTV equipment must act in accordance with the appropriate standards of probity and Council's Code of Conduct or be subject to disciplinary action.

10.1.10. A register will be kept detailing all instances of access to the security control systems.

10.1.11. All staff, including contractors, involved in the implementation, monitoring and management of Council's CCTV operations are also required to adhere to all policies and procedures adopted by Council, in particular Council's Code of Conduct.

11. Use of Artificial Intelligence in CCTV Systems

11.1. Council may, at its discretion, implement artificial intelligence (AI) technologies within CCTV systems to enhance monitoring capabilities, such as automated motion detection, object recognition, or behavioural pattern analysis. Any use of AI will be governed by relevant legislation, Council's privacy obligations, and ethical standards.

11.2. Where AI is used, it will operate under strict controls to ensure transparency, accountability, and the protection of individual privacy. Council will regularly review the use of AI technologies to ensure they remain appropriate, proportionate, and aligned with community expectations.

12. Recording of Material

12.1. Staff associated with CCTV operations will be made aware that recordings are subject to random audit and that they may be required to justify their interest in particular members of the public or premises.

12.2. Access to and use of recorded material will only take place:

12.2.1. In compliance with the needs of Police in connection with the investigation of a crime.

12.2.2. If necessary for the purposes of legal proceedings as ordered by a court of law.

12.2.3. For an internal review in the investigation of breaches of Council's Code of Conduct.

12.2.4. For an investigation of Council's liability for public damages or injuries.

12.2.5. For an investigation of damage to Council properties.

12.2.6. For an investigation of events contributing to the injury of Council employees or other Workers in accordance with the Workplace Surveillance Protocol.

12.2.7. For legitimate operational reasons, such as investigating incidents, ensuring safety, site management and security, work progress monitoring, intelligent video analytics, or supporting authorised audits and compliance checks.

12.3. Appropriate security measures will be implemented to protect against unauthorised access to, alteration, disclosure, loss, or destruction of recorded material.

12.4. Recorded material will be treated according to all relevant or appropriate legislation and standards, to provide continuity of evidence and to avoid contamination of evidence.

12.5. All relevant recorded material will be subject to random inspection by the audit team.

12.6. Recorded information will not be sold or used for commercial purposes or the provision of entertainment.

13. Public Access to CCTV Footage

13.1. In accordance with the Privacy and Personal Information Protection Act 1998 (Information Protection Principle No 11) the collection and use of CCTV recordings is undertaken only for the purposes as outlined in Section 12.2 of this Policy.

13.2. As CCTV footage may contain the personal information of individuals access to such information will not be made available to members of the public.

13.3. Should a member of the public be aware of the occurrence of a criminal activity that may have been recorded by a Council CCTV they should immediately report the matter to the NSW Police who will consider the appropriateness of seeking access to such CCTV footage in line with the requirements of this Policy and their policing obligations.

13.4. Access to recorded material may also be available in response to a Court issued Subpoena.

14. Data Breach Management

14.1. In the event of a suspected or confirmed data breach involving surveillance footage or related systems, Council will respond in accordance with its established Data Breach Policy. This includes assessing the nature and extent of the breach, containing the incident, and notifying affected parties where required.

14.2. Council reserves the right to take appropriate remedial and disciplinary action and may retain relevant footage or data for longer periods to support investigations or legal processes. All employees must immediately report any data breach or suspected breach to their supervisor or the designated Privacy Officer.

15. General

15.1. Council's CCTV systems will comply with the required Privacy Protection Principles as set out in the *Privacy and Personal Information Protection Act 1998* which provides for the protection of personal information, and the privacy of individuals generally.

15.2. Complaints about the operation of the CCTV system shall be reviewed in accordance with Council's Complaints and Feedback Management Policy and as required with Council's Code of Conduct.

16. Records Management

16.1. Staff will maintain all records relevant to administering this Policy in accordance with Council's Information and Records Management Policy.

16.2. Footage will only be released in accordance with the conditions outlined in this Policy.

16.3. All CCTV footage will be stored in a secure location that is inaccessible to the public. Footage will be retained for a minimum of 31 days in accordance with Council's standard retention practices. However, at Council's discretion, footage may be retained for longer periods where necessary to support operational needs, legal requirements, or investigations.

17. Compliance

17.1. Audits to review monitoring arrangements for CCTV operations will be undertaken periodically.

18. Breaches of Policy

18.1. Breaches of this Policy will be dealt with in accordance with Council's Code of Conduct and procedures for the administration of Council's Code of Conduct.

18.2. Breaches will be advised to the Chief Executive Officer and/or Director, via the Unit Manager, Projects and Asset Management, where appropriate.

19. Policy Definitions

Act	means the *Local Government Act 1993* (NSW)
AI	means Artificial Intelligence
Authorised Officer	means a person appointed or designated by a government agency or regulatory body to perform specific compliance and enforcement duties under a particular law or Act. They are granted powers to carry out functions outlined in that legislation, often including entry, inspection, and enforcement actions.
CCTV	means Closed Circuit Television
Council	means Central Coast Council
Contractor	means an individual or organisation engaged by Council to perform work or provide services on Council's behalf, whether under a contract, agreement, licence or other arrangement, who is not a direct employee of Council.
LGA	means Local Government Area
Operational purpose	means the use of CCTV systems to support the day-to-day functioning, safety, and security of Council-managed sites, facilities and services.
Policy	means Closed Circuit Television Policy

20. Policy Administration

Business Group	Infrastructure Services
Responsible Officer	Unit Manager, Projects and Asset Management
Associated Procedure (if any, reference document(s) number(s))	<<Enter text…>>
Policy Review Date	2029
File Number / Document Number	D16231731
Relevant Legislation (reference specific sections)	This Policy supports Council's compliance with the following legislation: ▪ Government Information (Public Access) Act 2009 ▪ Local Government Act 1993 ▪ Privacy and Personal Information Protection Act 1998 ▪ Privacy and Personal Information Protection Regulation 2019 ▪ Privacy Code of Practice for Local Government (2000) ▪ Security of Critical Infrastructure Act 2018 (Cth) ▪ State Records Act 1998 ▪ Surveillance Devices Act 2007 ▪ Workplace Surveillance Act 2005
Link to Community Strategic Plan	Theme 4: Responsible **Goal G: Good governance and great partnerships** B-A4: Enhance community safety within neighbourhoods, public spaces and places.
Related Policies / Protocols / Procedures / Documents (reference document numbers)	▪ AS/NZS 62672.1.2:2020 Video Surveillance Systems for use in Security Applications ▪ Australian Standard AS 4806.1-2006: Closed Circuit Television (CCTV) ▪ Council's Code of Conduct ▪ Delegations Register ▪ Information and Records Management Policy (D14025241) ▪ Council's Data Breach Policy ▪ Workplace Surveillance Protocol ▪ NSW Government Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television (CCTV) in Public Spaces (2014)

21. Policy Authorisations

No.	Authorised Function	Authorised Business Unit / Role(s)
1.	Use of CCTV in public spaces	Unit Manager, Projects and Asset Management Section Manager, Facilities Management and Operations Facility Manager, Facilities Management and Operations
2.	Access to recorded material	Unit Manager, Projects and Asset Management Section Manager, Facilities Management and Operations Facility Manager, Facilities Management and Operations
3.	Viewing of recorded material	Unit Manager, Projects and Asset Management Section Manager, Facilities Management and Operations Facility Manager, Facilities Management and Operations
4.	Oversight of CCTV system ownership, system access levels, approval workflows, and system audit support.	Chief Technology Officer, Information & Technology (as Platform and System Owner) Unit Manager, Projects and Asset Management (Business Owner)
5.	Use of CCTV for Operational purpose	Business Strategy and Performance Unit Customer Service Team Education and Care Team Holiday Parks Team Leisure and Pools Team Network Operations and Maintenance Team Parking Stations Team Waste Facilities Team
6.	Granting access to internal requests for footage	Chief Executive Officer Unit Manager, People and Culture Disclosures and Investigations Coordinator
7.	Granting access for operational purposes and activities	Unit Manager, Projects and Asset Management Section Manager, Facilities Management and Operations

8.	Reviewing and authorising public requests for access to CCTV footage	Unit Manager, Projects and Asset Management Section Manager, Facilities Management and Operations Facility Manager, Facilities Management and Operations
9.	Reviewing and authorising Government Agency requests for access to CCTV footage	Unit Manager, Projects and Asset Management Section Manager, Facilities Management and Operations Facility Manager, Facilities Management and Operations

22. Policy History

Revision	Date Approved / Authority	Description Of Changes
1	<<Enter text...>>	<<Enter text...>>
2	<<Enter text...>>	<<Enter text...>>