
CLOSED CIRCUIT TELEVISION (CCTV) POLICY

PURPOSE

The intention of this policy is to outline how Cook Shire Council (Council) will manage its obligations to the public and Cook Shire employees when installing, operating and managing its CCTV systems.

Council's primary reason for the installation and use of CCTV systems is to discourage and identify unlawful behaviour in and around Council property and in identified high-risk public spaces thereby enhancing the safety and security of the Shire's community and assets.

SCOPE

This policy applies to Council controlled and managed CCTV systems installed within its premises and in public spaces.

This policy applies across Council:

1. *to all Council employees and contractors and other parties involved with the installation, management and maintenance of Council's CCTV cameras, and who may access footage from time to time.*
2. *to any CCTV system installed and owned and operated by Cook Shire Council at any location within the Cook Shire Council local government jurisdiction, whether as one fully integrated system linking all towns across the shire or as separate individual stand-alone systems, and includes both mobile and fixed CCTV equipment, however does not apply to the operation and administration of:*
 - a. *BWC (Body Worn Camera) systems;*
 - b. *covert camera surveillance devices lawfully deployed for investigative purposes, e.g., gathering of evidence for enforcement of a Local Law.*

This policy should be read in conjunction with Council's Closed-Circuit Television (CCTV) System Administrative Instruction (*Currently being developed in support of operational practices for installation, configuration, and maintenance*)

Document Number:	D23/11977	<u>CONTROLLED DOCUMENT</u> This electronic document is guaranteed as the most current. DO NOT COPY. Unauthorised hard copies of this document are prohibited.	Page 1 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

DEFINITIONS

TERM	DEFINITION
Access	The act of viewing and copying, with approval, CCTV footage.
CCTV System	All video capture and storage apparatuses, network devices, and network infrastructure that functions as part of closed-circuit television.
ICT	Council's Information and Communications Technology Department
Information Privacy Principles	Principles that have been adopted by the Queensland government from the Commonwealth Privacy Act 1988 that have the same force and effect as sections in legislation.
Legislation	As itemised in this policy and as applicable to the management of CCTV systems.
Personal information	Information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion and can include still images or video footage of an individual.
Premises and public spaces	Any location where a CCTV system is installed and includes any place that the public may access by right or by invitation, whether express or implied and whether or not a charge is made for admission to the place. Premises and public spaces include public streets, public parks, public halls, museums, galleries, aquatic centres, sports grounds, roads and other traffic ways and libraries.
Shire assets	Assets refer to assets and infrastructure owned or controlled by Council.

POLICY STATEMENT

Council endeavours to protect the Shire's assets, employees and the community with a range of initiatives including the installation of CCTV systems in public spaces.

Document Number:	D23/11977	<p>CONTROLLED DOCUMENT</p> <p>This electronic document is guaranteed as the most current. DO NOT COPY.</p> <p>Unauthorised hard copies of this document are prohibited.</p>	Page 2 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

OBJECTIVE

CCTV systems controlled by Council will be installed and managed in accordance with applicable legislation, in support of achieving the following objectives only:

1. The identification, management and deterrence of criminal or unlawful behaviour.
2. The identification of perpetrators in support of prosecution of criminal offences.
3. Contribute to an integrated multi-agency approach to crime prevention and community safety.
4. The protection of Council's assets and investigation into matters relating to asset.
5. In provision of information relating to a work health and safety investigation.
6. The identification of risk to the public, assets and Council employees.
7. Obtain road/traffic data including license plate recognition access support to Queensland Police.
8. Obtain information in relation to road conditions, for example, the monitoring of water levels at river and creek crossings to determine if roads remain traversable.

ETHICAL SYSTEM MANAGEMENT

In managing the CCTV system, Council will:

1. Ensure the management of each CCTV system is consistent with the purpose of the system;
2. Manage each CCTV system in accordance with Australian legislative requirements and standards; and
 - i. In accordance with the processes described in Council's Closed-Circuit Television (CCTV) System Administrative Instruction; and
 - ii. In accordance with the Articles of Human Rights and the Human Rights Act 2019.
3. Not engage in general surveillance of the public or employees, or repurpose, or allow another party to use or access the CCTV system in such a way that it contravenes any legislative obligation.

GENERAL PRINCIPLES

Data recorded on Council's CCTV system shall only be used for the purposes outlined in this policy and access to that information shall only take place in accordance with this policy.

Cameras will not be used to intentionally monitor adjacent or nearby premises or buildings, although it is acknowledged that data captured by the cameras will generally include some exterior vision of business or other premises.

Document Number:	D23/11977	<u>CONTROLLED DOCUMENT</u> This electronic document is guaranteed as the most current. DO NOT COPY. Unauthorised hard copies of this document are prohibited.	Page 3 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

Any person who uses the equipment for any reason other than as outlined in this policy will be subject to disciplinary and/or legal action.

The management and operation of the Cook Shire Council CCTV system will:

1. Be undertaken by authorised and appropriately trained Council officers.
2. Be in accordance with applicable privacy and recordkeeping legislation.¹
3. Comply with the principles of impartiality and integrity and operational and procedural efficiency.²
4. Acknowledge that personal protection has priority over property protection.
5. Have due regard to the privacy and civil liberties of individual members of the public, including the rights to freedom of religious and political expression and assembly.³
6. Ensure the disclosure of data is coordinated and controlled through a centralised point which accords with the provisions of current legislation⁴ and this policy.
7. All data will be managed in accordance with relevant ICT information access instruments.

PUBLIC TO BE NOTIFIED

Council will comply with privacy legislation with respect to making individuals generally aware of:

1. the purpose for the collection of their personal information
2. any lawful authority for the collection
3. to whom Council may pass the information onto
4. as appropriate, to whom the information may, in turn, be passed on to

MONITORING OF CAMERAS

Except where monitoring equipment associated with permanently fixed CCTV cameras is installed at a QPS facility under an MOU with QPS, such equipment will normally be installed at a secure Council administration centre or other available Council facility such as a library, depot or visitor information centre which meets the required security standards.

Where data is being recorded, live monitoring of any installed CCTV system will not typically be undertaken by Council with the exception of the instances where CCTV monitoring is used to assist in the performance of a work function. For example:

¹ See especially *Information Privacy Act 2009 (Qld)*, *Right to Information Act 2009 (Qld)*, *Public Records Act 2002 (Qld)*.

² See *Local Government Act 2009 (Qld)* s 13. See also *Public Sector Ethics Act 1994 (Qld)* ss 4-9.

³ See especially *Human Rights Act 2019 (Qld)*.

⁴ See especially *Information Privacy Act 2009 (Qld)*, *Right to Information Act 2009 (Qld)*.

Document Number:	D23/11977	CONTROLLED DOCUMENT This electronic document is guaranteed as the most current. DO NOT COPY. Unauthorised hard copies of this document are prohibited.	Page 4 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

1. A monitoring station secured in the ICT office providing images for the purpose of ensuring CCTV cameras are fully operational and functioning as intended.
2. A single camera feed that provides monitoring of traffic entering the Council depot facility by Councils Depot administrator for site traffic safety.
3. Data captured for road/traffic management and water level monitoring purposes, recorded data will only be viewed by Council in response to a valid disclosure application.

Where monitoring equipment is installed at a QPS facility under an MOU between Council and QPS, it is acknowledged that authorised QPS officers may undertake live monitoring of cameras.

RETENTION OF CAMERA SURVEILLANCE DATA

Where possible, recording equipment attached to any Council CCTV system will be set to a maximum 30 day overwrite cycle, meaning that data recorded (the primary image) will be available for retrieval and viewing for a period of up to 30 days after it has been initially captured and after that period will then be overwritten (erased) by new data captured by the CCTV cameras. This period may be reduced, based on the capacity of the system's storage device. In some instances, this period may not be user configurable and will default to the setting defined by the system. The exception to the above is:

1. where the recorded data contains images relevant to an incident in respect of which a Police investigation has been, or is to be, undertaken and the surveillance data is, or may be, required for evidentiary purposes in a Court proceeding.
2. where the recorded data contains images relevant to a breach of Council's local laws, or any other incident that requires further investigation, and Council may institute legal proceedings against the person/s who committed the breach.
3. where a valid application has been received for disclosure of data that is still within the applicable retention period and additional time is required to process the application and/or having processed the application, it is deemed appropriate to disclose the requested data to the applicant.

Where data is required to be kept for the purposes outlined above, it will be transferred from the Network Video Recorder (NVR) onto Council's approved evidence management system or, should the data size exceed the practical capacity to transfer/store the data on this system, retained on an appropriately secured storage device, and thereafter dealt with in accordance with the relevant current retention and disposal schedule issued by the State Archivist.

Where practical and possible, data that is retained shall only include that section of the NVR recording which shows the incident occurring with only those images prior to and after the incident necessary to show the incident as a whole.

Document Number:	D23/11977	<p>CONTROLLED DOCUMENT</p> <p>This electronic document is guaranteed as the most current. DO NOT COPY.</p> <p>Unauthorised hard copies of this document are prohibited.</p>	Page 5 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

DISCLOSURE OF PERSONAL INFORMATION TO OTHER AGENCIES/LEGALLY AUTHORISED PARTIES

Other than where disclosure is required by law, on application and with the prior written approval of the CEO or an authorised delegate, Council may permit the controlled disclosure of CCTV data that contains personal information to relevant agencies or legally authorised parties for the purposes of:

1. providing evidence in criminal proceedings
2. providing evidence in civil proceedings
3. the prevention of crime and disorder
4. the investigation and detection of crime (includes identification of offenders)
5. identification of witnesses
6. individual or public health, safety or welfare concerns Closed-Circuit Television (CCTV) System
7. the individual has expressly or impliedly agreed to the disclosure

COMPLAINTS

All complaints in relation to the CCTV system will be dealt with through the Council's adopted complaints management policy and investigated by the delegated Complaints Officer

PUBLIC ACCESS TO CCTV FOOTAGE

Access to footage is guided by the Information Privacy Act 2009 and the Right to Information Act 2009.

Generally, for members of the public, access to CCTV data must be made through a formal written order issued by a body with administrative or judicial jurisdiction for example court orders, warrants, prerogative writs and subpoenas.

Applications to view Council's CCTV data may be made by the police for the purpose of:

1. Providing evidence in criminal proceedings
2. Providing evidence in civil proceedings
3. The prevention and reduction of crime and disorder
4. The investigation and detection of crime (including identification of offenders)
5. Identification of witnesses.

Document Number:	D23/11977	CONTROLLED DOCUMENT This electronic document is guaranteed as the most current. DO NOT COPY. Unauthorised hard copies of this document are prohibited.	Page 6 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

KEY RESPONSIBILITIES

RESPONSIBLE OFFICER	RESPONSIBILITY
Chief Executive Officer	Responsible for the overall management and administration of Council's CCTV systems.
Council Employees	Familiarising themselves with this policy and understanding their obligations with reference to Council's CCTV systems.
Governance Coordinator	Applications for access to footage received under the Right to Information Act 2009; and Policy review and dissemination.
Information and Communications Technology (ICT) Officers	CCTV system management; The provision of ICT infrastructure appropriate for Council's CCTV systems; Providing approved access to footage, CCTV hardware and software security; and Digital storage of captured footage.
Records Management Officers	Responsible for the retention, classification, security and disposal of lawfully accessed footage in accordance with the Public Records Act 2009.

SPECIFIC RESPONSIBILITIES - APPOINTED PERSONS

The following responsibilities have been assigned by Council's Chief Executive Officer in relation to the CCTV system:

SPECIFIC RESPONSIBILITIES-	APPOINTED PERSONS
CCTV system management—system integrity and statutory compliance	<ul style="list-style-type: none"> The CEO is responsible for authorising the review, access, and release of any footage captured by the CCTV system. The CEO is responsible for ensuring that the system is operated in accordance with this policy and relevant legislation. Council's ICT Manager is responsible for ensuring the integrity of the system and in this regard may request the services of an external agency to audit the application of this policy and operating procedures.

Document Number:	D23/11977	<u>CONTROLLED DOCUMENT</u> This electronic document is guaranteed as the most current. DO NOT COPY. Unauthorised hard copies of this document are prohibited.	Page 7 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

CCTV system management—system integrity and statutory compliance	<ul style="list-style-type: none"> • Council's ICT Coordinator will oversee the processing of any data for release as requested under the information privacy and access legislation. • Council's Governance Coordinator will endorse any data for release as requested under the information privacy and access legislation. That endorsement will ensure that the provisions of the aforementioned Acts have been met. • Appropriately licensed and trained ICT staff will be responsible for initial viewing of recorded data to locate requested data of a reported incident, appointed by the ICT Manager with the approval of the CEO. • Any requests for access to data that do not fall within the principles outlined in this policy will be referred to Council's legal advisers.
Maintenance and Technical Support Services	<ul style="list-style-type: none"> • The ICT Department is appointed to assume responsibility for in-house technical support to the CCTV system and general maintenance and configuration of the supporting network.

REFERENCES, LEGISLATION AND GUIDELINES

Queensland Local Government Act 2009 and Local Government Regulation 2012

Queensland Public Records Act 2009

Queensland Right to Information Act 2009

Queensland Information Privacy Act 2009

Commonwealth Privacy Act 1988

Employee COC; Councillor COC; Complaints; and CCTV Administrative Instructions

Evidence Act 1977 (QLD)

Human Rights Act 2019 (QLD)

Public Sector Ethics Act 1994 (QLD)

Document Number:	D23/11977	<p>CONTROLLED DOCUMENT</p> <p>This electronic document is guaranteed as the most current. DO NOT COPY.</p> <p>Unauthorised hard copies of this document are prohibited.</p>	Page 8 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

RELATED DOCUMENTS

- CSC Closed-Circuit Television (CCTV) System Administrative Instruction
- CSC Information Security Policy
- CSC ICT Strategic Plan 2021-2025

IMPLEMENTATION AND COMMUNICATION

Once adopted, this policy will be:

1. Published on Council's website;
2. Made available to all Councillors and employees through various communication channels;
3. Distributed to relevant State Agencies as required; and
4. Provided to all parties who apply for access to footage.

APPROVED BY

Council Resolution 2023/142

THIS POLICY IS TO REMAIN IN FORCE UNTIL OTHERWISE DETERMINED BY EXECUTIVE MANAGEMENT

REVIEW

SPONSOR:	Director Organisational Business Services
OFFICER RESPONSIBLE FOR REVIEW:	Governance Coordinator
ADOPTION DATE:	27 June 2023
REVIEW DATE:	June 2026

Document Number:	D23/11977	CONTROLLED DOCUMENT This electronic document is guaranteed as the most current. DO NOT COPY. Unauthorised hard copies of this document are prohibited.	Page 9 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		

AMENDMENT HISTORY

VERSION	AMENDMENT DETAILS	AMENDMENT DATE	APPROVAL
v1	New Policy	December 2020	Resolution 2020/314
v2	Review by ICT Coordinator - Amendments	June 2023	Resolution 2023/142

Document Number:	D23/11977	<p>CONTROLLED DOCUMENT</p> <p>This electronic document is guaranteed as the most current. DO NOT COPY.</p> <p>Unauthorised hard copies of this document are prohibited.</p>	Page 10 of 10
Authorised By:	Council Resolution 2023/142		
Original Issue Date:	December 2020		
Last Modified:	June 2023		
Review Date:	June 2026		
Current Version:	2.0		