2022

THE LEGISLATIVE ASSEMBLY FOR THE

AUSTRALIAN CAPITAL TERRITORY

CLOSED CIRCUIT TELEVISION (CCTV) POLICY

Presented by
Shane Rattenbury MLA
Attorney-General
August 2022

ACT Government

CLOSED-CIRCUIT TELEVISION (CCTV) POLICY

ISSUE DATE:

AUGUST 2022

CONTENTS

ACKNOWLEDGEMENT OF COUNTRY

The Australian Capital Territory and the broader Canberra Region is Ngunnawal Country. It represents an important meeting place for the Ngunnawal people and those from other Aboriginal Nations.

The ACT Government acknowledges the Ngunnawal people as the traditional custodians of this land, and pays respect to Ngunnawal elders, both past, present and emerging for their contribution to the life and culture of Canberra.

The ACT Government also pays its respects to other Aboriginal and Torres Strait Islanders.

ACCESSIBILITY

The ACT Government works to make its information, services, events and venues as accessible as possible.

If you have difficulty reading a standard printed document and would like to receive this publication in an alternative format, such as large print, please phone Access Canberra on 13 22 81 or email the Justice and Community Safety Directorate at jacssemd@act.gov.au.

If English is not your first language and you require a translating and interpreting service, please phone 13 14 50. If you are deaf, or have a speech or hearing impairment, and need the teletypewriter service, please phone 13 36 77 and ask for Access Canberra on 13 22 81.

For speak and listen users, please phone 1300 555 727 and ask for Access Canberra on 13 22 81. For information on these services visit www.relayservice.com.au.

CONTACT

Security and Emergency Management Division
Justice and Community Safety Directorate
ACT Government

Tel: +61 2 6205 4795

Email: JACSSEMD@act.gov.au

Mail: GPO Box 158, Canberra City, ACT 2601

ATTORNEY-GENERAL'S FOREWORD

I am pleased to present the *Closed-Circuit Television (CCTV) Policy* (the CCTV Policy) on behalf of the ACT Government.

The ACT Government has a focus on ensuring that Canberra remains a safe, vibrant, and cohesive city for residents and visitors. Everyone has a right to feel safe as they move around our city and engage with the ACT's many public spaces, venues, and events.

To support this outcome, the ACT Government has adopted CCTV as a key part of its safety and security approach. CCTV is installed in many ACT Government facilities, vehicles and open spaces for public safety, traffic and asset monitoring and a range of other purposes.

The ACT Government recognises the potential privacy implications of the use of CCTV technologies. This CCTV policy provides governance and administration of CCTV technologies which balances the need and purpose for CCTV with the right to privacy.

This CCTV Policy outlines measures that ACT Public Sector agencies must take to ensure people are notified where CCTV is in use, and requires ACT Government Directorates to provide access to policy statements that set out how CCTV footage is managed. Through this CCTV policy, the community can have visibility of, and confidence in the use, collection and disclosure of CCTV footage within the ACT Government.

Shane Rattenbury MLA

Attorney-General

DEFINITION OF TERMS

Term	Definition
Agency Security Advisor (ASA)	The official responsible for day-to-day management and operation of public sector agency protective security. ASAs are also responsible for ensuring that staff members are aware of security practices and procedures relevant to their workplace, training, and regular testing of security arrangements.
Biometrics	Biometrics is the process capable of performing large-scale identification, verification, and authentication functions – these functions can be used to identify an individual and associated individual's details and history. The ACT Government Public Safety Network (the Network) will not hold this information.
Closed-Circuit Television (CCTV)	A television system intended for only a limited number of viewers. This definition is inclusive of recording equipment (analogue or digital), display equipment, transmission systems, transmission media, optical recording devices, and interface control. This does not include portable or fixed speed and red-light cameras; movable surveillance cameras where images are saved to external storage devices and not broadcast; or the use of cameras and similar equipment by the broadcast media for the purposes of journalism, education, public information, artistic or literary purposes.
CCTV system	A network of Closed-Circuit Television (CCTV) cameras owned by an ACT public sector agency, as a temporary, mobile or permanent installation. This may include the cameras that are attached to the Network Video Recorder (NVR) which captures the images.
Digital, Data and Technology Solutions (DDTS)	DDTS provides information and communications technology (ICT) and allied services to directorates, including infrastructure, applications support, development, ICT policy and project services.
Must	Something that is mandatory.
NVR	Network Video Recorder - the main device that holds the images and footage of events being recorded.
Recorded images	Any images captured by CCTV systems operated and maintained by an ACT Government Directorate.
Should	Something that is recommended.

1. PURPOSE

1.1. This policy establishes whole of government arrangements for CCTV governance, installation, and operation.

1.2. This policy supersedes and makes redundant the *ACT Government Code of Practice for Closed-Circuit Television Systems* (2009).

1.3. Under this policy, directorates:

a. must incorporate collection and management of CCTV into their Privacy Statement as required under *Territory Privacy Principles* (TPP) 1 in the *Information Privacy Act 2014*. This includes the information required by section 6.3.1. of this policy

b. must identify in their Privacy Statement how the directorate will manage personal information captured through CCTV and notify a person that their personal information is being collected

c. must develop plans and procedures specific to their needs, to ensure consistency through all ACT Government environments, provided they are not in conflict with any aspect of this policy.

2. SCOPE

2.1. This policy applies to all ACT public sector agencies.

2.2. This policy does not apply to:

- Camera systems used to detect traffic infringements.
- Time-lapse cameras in public places by the ACT Government associated with monitoring infrastructure projects.
- Body Worn Camera use when recording audio conversations, which must comply with the *Listening Devices Act 1992*. Visual recordings, without sound, should be managed in accordance with this policy.
- ACT Policing in car camera systems and the Automatic Number Plate Recognition System (ANPR).
- Camera systems used by ACT Corrective Services for monitoring and safety, these systems are managed in accordance with the *Corrections Management Act 2007.*
- Camera systems used by ACT Courts and Tribunals for monitoring and safety, these systems are managed under the jurisdiction of the court.
- Camera systems used by the ACT Legislative Assembly for monitoring and safety, these systems are managed under the jurisdiction of the Assembly.
- Camera systems used for wildlife monitoring purposes or gathering of information for statistical purposes particular to land use activities for land use monitoring, unless the camera has recorded information that may be relevant to the investigation of a crime.
- Camera systems which capture information that constitute a 'health record' under the *Health Records (Privacy and Access) Act 1997*. For example, these camera systems may be used as part of health clinical services for patient monitoring and safety such as medical services associated with radiation treatment and Magnetic Resonance Imaging (MRI) scanning.

- Camera systems used as part of a tenancy or retail arrangement, not owned, or operated by the ACT Government, who have a standalone or independent system.

2.3. CCTV will not be installed in prohibited areas as defined under section 41 of the *Workplace Privacy Act 2011.* The ACT Public Service *Workplace Privacy Policy Statement & Notice to Workers* sets out the policy in relation to workplace surveillance applicable to all ACT Government workers and contractors.

3. BACKGROUND

3.1. Under the *Information Privacy Act 2014*, an agency may collect personal information only if it is reasonably necessary for, or directly related to, one or more of the agency's functions or activities.

3.2. Each directorate will need to consider the purpose for each CCTV system. Generally, directorates may install and operate a CCTV system for one or more of the following purposes:

a. crime deterrence, investigation and evidence to support criminal proceedings

b. asset monitoring and security

c. access control monitoring

d. public safety and/or event monitoring

e. enhancing the response to and management of incidents and emergencies

f. regulatory enforcement and evidence for use in court proceedings

g. training, education and community engagement purposes

h. traffic, vehicle and parking management.

3.3. Should a directorate seek to install and operate a CCTV system for purposes other than those outlined above, special consideration must be given to the purpose of the system to ensure that it is reasonably necessary for or directly related to one of the directorate's functions or activities.

3.4. Directorates must develop an internal project proposal for new CCTV installations (unless it is an expansion of a previously agreed installation) for approval by an appropriate authority within the directorate who can authorise the proposal as compliant with ACT legislation referred to in this policy. The proposal should include the following points:

a. clearly articulates the purpose/s of the system as outlined at section 3.2 or 3.3

b. has a cost benefit analysis and review timeline for the system

c. identifies if a permanent, mobile or temporary installation will be installed

d. provides procurement and ongoing maintenance costs, including licencing

e. identifies who will access the systems and how this is audited

f. identifies how data will be stored and destroyed

g. considers and identifies the right to privacy and human rights, including undertaking an analysis of whether the CCTV project proposed is reasonable and proportionate to its aim

h. articulates the procedure for third party access to data.

4. PRIVACY AND HUMAN RIGHTS

4.1. CCTV systems must be operated with proper consideration to privacy and human rights. The ACT Government recognises that the operation of CCTV systems and the use, collection and disclosure of CCTV footage will engage and may limit the right to privacy under section 12 of the *Human Rights Act 2004.*

4.2. Directorates must undertake the use, collection and disclosure of CCTV footage in accordance with the *Information Privacy Act 2014* to ensure compliance with the right to privacy.

4.3. Directorates must operate CCTV systems in a manner that restricts viewing of footage to those with a need to know.

4.4. CCTV systems must not be used for the purpose of automated biometric verification or biometric identification.

5. PUBLIC SAFETY CCTV NETWORK (THE NETWORK)

5.1. The Network is an ACT Government-owned network of interconnected CCTV systems located at various public venues and open spaces. The purpose of the Network is to support public safety monitoring, resource management, emergency response and for criminal investigation and prosecution purposes.

5.2. Live and recorded footage from the CCTV Network is available to Government and ACT Policing.

5.3. Directorates may elect for their CCTV systems to be connected to the Network, and for live and recorded CCTV information to be available to ACT Policing under the provisions of an Agreement or Memorandum of Understanding between the Territory and ACT Policing.

5.4. Where a CCTV system is connected to the Network, directorates must take actions, including in their Privacy Statement, to make a person reasonably aware that live and recorded CCTV footage is provided to ACT Policing.

6. CCTV GOVERNANCE

6.1. PROTECTIVE SECURITY WORKING GROUP (PSWG)

6.1.1. The objectives of the PSWG includes to:

a. identify and progress measures to enhance CCTV capability to support business needs

b. maintain and develop whole of government policy and procedures to support the compliance and good governance of CCTV

c. identify and progress measures enhancing the efficiency of CCTV utilisation and procurement

d. identify and progress collaborative approaches towards CCTV asset planning and replacement, including budget initiatives

e. support and coordinate advice and reporting to government through the Security and Emergency Management Policy Group, including the provision of an annual statement of CCTV utilisation

f. progress the implementation of actions identified in the *Strategic Closed-Circuit Television (CCTV) Plan 2020-2022* and any subsequent plans, initiatives, reviews and audits

g. support the identification of ICT requirements to support CCTV (coordinated by DDTS)

h. progress the establishment of a CCTV panel of contractors, consultants, providers and other related whole of government procurement

i. share advice and lessons learnt on previous and upcoming projects.

6.2. KEY ROLES AND RESPONSIBILITIES

Role	Responsibilities
Security and Emergency Management Division (Justice and Community Safety Directorate – JACS)	• Lead and coordinate the development of whole of government approaches to CCTV policy, strategy, standards, procurement of services and programs. • Support and coordinate the functions of the PSWG. • Support Agency Security Executives and Agency Security Advisors with policy compliance requirements. • Provide advice on proposed CCTV installations.

Chief Minister, Treasury and Economic Development Directorate	• Digital, Data and Technology Solutions (DDTS)
	  ○ Provide strategic advice and operational support to the networking of CCTV systems.
	  ○ Coordination of requests for footage made to Access Canberra.
	• Access Canberra
	  ○ Provide and maintain systems to receive and log requests for CCTV footage from third parties.
	  ○ Enquiries should be made by contacting Access Canberra on 13 22 81.

Transport Canberra and City Services Directorate (TCCS)	• Maintain a Whole of Government CCTV location site map database. • Maintain the Whole of Government CCTV third party request database. • Contact point for urgent CCTV footage requests from an ACT Government system. • Receive, assess and distribute third party CCTV requests to responsible ACT Government agencies for action.

6.3. CCTV SYSTEMS REGISTERS

6.3.1. Directorates must:

a. establish and maintain a register of all CCTV systems under their control

b. publish information about the use, operation and purpose of the cameras in their Privacy Statement

c. ensure current CCTV system registers are provided to TCCS for inclusion in the whole of government CCTV register and database.

6.3.2. The register must include at a minimum:

a. the manufacturer and system type

b. the purpose/s of the system

c. the location of the system

d. the number of cameras on the system

e. the signage used to notify persons of the system

f. if the recorded information is disclosed to another entity, include the name of that entity.

6.3.3. When requested, directorates must provide a copy of their register to SEMD, JACS.

7. CCTV INSTALLATION AND OPERATION

7.1. NEW INSTALLATIONS

7.1.1. CCTV is a proven and effective technology that can be used for a wide range of purposes but can be costly to install and maintain. Without proper selection, design and maintenance it can also be ineffective and unreliable. Prior to the drafting of a proposal, early engagement with DDTS and SEMD is critical.

7.1.2. To ensure that a CCTV system is fit for purpose, directorates should seek professional and qualified assistance to ensure the CCTV system will meet the desired business and security outcomes.

7.1.3. In a project proposal, directorates must document:

a. the purpose of CCTV as identified in 3.2 or 3.3 in this policy and whether it is the best value solution to achieve the business requirement, consulting with SEMD and DDTS

b. that the installation complies with legislation and relevant Standards, including but not limited to:

- *Human Rights Act 2004*
- *Workplace Privacy Act 2011*
- DDTS installation standards
- Installation standards of the relevant vendor and product provider.

c. consultation with SEMD, TCCS Security and the PSWG Chair of the planned installation of the CCTV system.

7.2. NOTIFYING THE COMMUNITY OF CCTV SYSTEM INSTALLATION

7.2.1. Directorates must notify the community where a new CCTV system is being installed in a public space.

7.2.2. This notification must occur through one or more of the following mechanisms:

a. signage in the area where the CCTV is to be installed

b. ACT Government communication channels

c. advice to the respective Community Council.

7.3. NOTIFYING PEOPLE OF CCTV SYSTEM PRESENCE

7.3.1. Directorates must take reasonable steps to notify people when they are entering an area where CCTV systems are operating.

7.3.2. Directorates must also notify the public of the use and operation of a CCTV system and the purpose of the system in a Privacy Statement.

7.3.3. This notification will normally occur using appropriate signage which must be prominently and clearly displayed. The signage must include:

a. whether the recording of CCTV footage is continuous or limited; and

b. the purpose of the CCTV; or

c. information which enables a person to easily find out the purpose of the CCTV, for example a link to a website with relevant information, or to the Privacy Statement.

7.4. CCTV SYSTEM SECURITY

7.4.1. Directorates must implement controls to protect access to a CCTV system. This must include:

a. establishing physical security arrangements to protect the system from unauthorised access or viewing

b. password protecting access to linked software applications and audit capability to track users

c. ensuring the capabilities to view and copy recorded footage are only available to those who are authorised

d. undertaking audits/compliance reviews of CCTV systems.

7.5. CCTV SYSTEM MAINTENANCE

7.5.1. CCTV systems require programmed inspection and maintenance. Directorates should ensure that footage captured via CCTV systems is of sufficient quality to be accurate, up-to-date and complete. When recording, this requires CCTV footage to be collected consistently to prevent gaps in the footage.

7.5.2. Directorates must ensure CCTV systems under their control are checked for proper performance and maintained at regular intervals.

7.5.3. Checks and maintenance must include:

a. Cameras – cleanliness, focus and operation

b. Software – patched, updated and time synchronisation

c. Recordings – maintained pursuant to the *Territory Records Act 2002*

d. Signage – current and visible at all times

e. Licence configuration and planning.

7.5.4. Network Video Recorders (NVRs) must be life cycled, budgeted for and upgraded when required.

7.6. CCTV SYSTEM REMOVAL

7.6.1. Directorates must decommission and remove CCTV systems when the business requirement is no longer present. If it is financially unviable or impracticable to remove a CCTV system, it must be decommissioned, and this must be documented.

7.6.2. The decommissioning or removal of a CCTV system must include the destruction of camera devices and the removal of optical recording devices and associated signage in accordance with the relevant DDTS/directorate policy.

7.6.3. All CCTV data from a decommissioned system must be managed in accordance with the *Territory Records Act 2002.*

8. CCTV INFORMATION MANAGEMENT

8.1. All use and disclosure of CCTV information by a directorate must comply with TPP 6 in the *Information Privacy Act 2014*.

8.2. Directorates must develop processes and procedures for intra and inter-directorate sharing of CCTV footage. Where a directorate intends to routinely disclose information to a different entity, this must be notified to the public in a Privacy Statement.

8.3. CCTV SYSTEM REQUESTS

8.3.1. All requests for CCTV information, excluding Freedom of Information (FOI) applications and subpoenas, must be lodged with Access Canberra (13 22 81).

8.3.2. Once logged, all requests will be reviewed for completeness and accuracy by TCCS and then assigned to the relevant CCTV system owner for actioning (viewing, recording or release where possible).

8.4. REQUESTS FOR INFORMATION

8.4.1. A person may request access to their personal information under the *Information Privacy Act 2014.*

8.4.2. CCTV footage is subject to the provisions of the *Freedom of Information Act 2016.* Third party requests for CCTV footage must be lodged and managed in accordance with a directorate's FOI arrangements.

8.5. DATA RETENTION

8.5.1. The *Territory Records Act 2002* establishes the legal requirements for directorates to manage CCTV records, including but not limited to:

a. storage

b. retention and disposal in accordance with the *Territory Records (Records Disposal Schedule – Security Coordination Records) Approval 2009 (No. 1)*

c. copying and release.

8.6. AUDITS

8.6.1. Directorates should implement appropriate assurance processes to ensure their CCTV systems are compliant with this policy, other linked ACT Public Service policies and relevant legislation.

8.6.2. Assurance processes should consider:

a. user access

b. system performance and maintenance

c. compliance with the *Information Privacy Act 2014* and the *Territory Records Act 2002*

d. management of CCTV requests and copied footage.

8.6.3. As best practice information sharing, directorates are encouraged to share the results of their assurance processes with the PSWG.

8.7. VIDEO ANALYTICS

8.7.1. CCTV end-user software has evolved to the point where video analytic capabilities are now offered as standard features.

8.7.2. Video analytics can automate many features that a CCTV operator may typically perform. This includes:

a. creating alerts if people or vehicles are in particular areas or behave in a particular way

b. searching recorded footage for people or objects.

8.7.3. In recognition of the benefit that video analytics provides to public safety and the investigation of crime, the ACT Government will use video analytics under specified and approved conditions. Such as a system automated search for a specific entity versus an officer manually searching the same footage.

8.8. TRAINING

8.8.1. Directorates must ensure that training is provided to all employees responsible for the operation of the CCTV system and that the training is recorded.

8.8.2. Vendor training may be available online. Information on how to access vendor training should be shared through the PSWG and can be sought from SEMD.

8.8.3. Training must include as a minimum the following elements:

a. awareness of this policy and the TPPs

b. awareness, understanding and working knowledge of the directorate's CCTV policy and procedures with an emphasis on handing requests for access by other entities and under the *Freedom of Information Act 2016*

c. understanding of the procedures and requirements for viewing and retrieval of recorded footage

d. awareness of CCTV functions.

8.9. COMPLAINTS

8.9.1. Directorates will manage complaints about the use of their CCTV systems in accordance with their complaints management process.

9. NON-COMPLIANCE WITH THIS POLICY

9.1. Any misuse of a CCTV system is a security related incident and must be reported to the relevant Agency Security Adviser and as per directorate policy as soon as practicable.

10. REVIEW

10.1. This policy is due for review in 2024, or earlier where there are changes that affect the operation of the policy.

11. REFERENCES

11.1. The relevant legislation underlying this policy is:

a. *Human Rights Act 2004*

b. *Privacy Act 1988* (Cth)

c. *Information Privacy Act 2014* and the *Territory Privacy Principles* (**TPPs**)

d. *Public Sector Management Act 1994*

e. *Territory Records Act 2002*

f. *Workplace Privacy Act 2011*

g. *Listening Devices Act 1992*

h. *Road Transport (Public Passenger Services) Regulation 2002*

i. *Health Records (Privacy and Access) Act 1997*

j. *Freedom of Information Act 2016.*

AMENDMENT HISTORY

Version	Issue Date	Amendment Details	Author (Position)
1.0	[MONTH] 2022	New policy	Senior Director Protective Security Policy