

# Policy

## Closed Circuit Television (CCTV)



## Document information

<b>Security classification</b>	<b>OFFICIAL</b>		
<b>Date of review of security classification</b>	Every three years		
<b>Approving Officers</b>	Belinda Zieth, Principal Executive Officer, Right to Information and Privacy, Strategic Policy and Legal Services Michelle Duckworth, Director, Right to Information and Privacy, Strategic Policy and Legal Services Leanne Robertson, Assistant Director-General, Strategic Policy and Legal Services		
<b>Authority</b>	David Mackie, Director-General, Department of Justice and Attorney-General		
<b>Documentation status</b>		<input type="checkbox"/> Consultation release	<input checked="" type="checkbox"/> Final version
<b>Next review date</b>	15 March 2024		
<b>Document reference</b>	<b>eDOCS number: 5683431</b>		

## Version history

<b>Version</b>	<b>Notes</b>	<b>Changed by and date</b>
1.0	Version 1 (eDOCS number 3668087) Effective August 2018	Senior Project Officer, Right to Information and Privacy, Strategic Policy and Legal Services
2.0	Version 2 (eDOCS number 5683431) Review and edit Effective 15 March 2023	A/Senior Project Officer, Right to Information and Privacy, Strategic Policy and Legal Services

## Policy owner/enquiries

All enquiries regarding this document should be directed in the first instance to the Director, Right to Information (RTI) and Privacy, Strategic Policy and Legal Services, Department of Justice and Attorney-General.

This policy is owned by the Director, RTI and Privacy who is responsible for the development and ongoing review of the policy.

## Policy approval and review

This policy version 2.0 was approved by the Director-General, Department of Justice and Attorney-General on 15 March 2023.

This policy is reviewed every three years to ensure that it is compliant and relevant to the ongoing needs and uses of CCTV within DJAG. It will also be evaluated in line with changes to business and information security risks to reflect the current agency risk profile. Any review of this document should identify whether the purpose of the policy continues to be relevant and lawful and that the policy achieves its objectives. The next scheduled review is 15 March 2024.

This policy may also be updated at the discretion of RTI and Privacy if it is identified that changes need to be made to reflect the evolving nature of DJAG's work. RTI and Privacy will coordinate any review of this policy which is undertaken in the future. Consultation during any review will occur as required.

## **Security classification**

This document has a security classification of OFFICIAL.

## **Licence**

Closed Circuit Television (CCTV) policy © The State of Queensland (Department of Justice and Attorney-General) 2023.



This work is licenced under a Creative Commons Attribution 4.0 International Licence.

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as OFFICIAL and will be managed according to the requirements of the QGISCF.

## Table of contents

<i>Document information</i> .....	2
<i>Version history</i> .....	2
<i>Policy owner/enquiries</i> .....	2
<i>Policy approval and review</i> .....	2
<i>Security classification</i> .....	3
<i>Licence</i> .....	3
1. Purpose.....	6
2. Policy Statement.....	6
3. Principles .....	6
4. Application.....	7
5. Identifying CCTV system ownership .....	7
5.1 Usage and ownership.....	7
5.2 Co-location.....	7
6. Procedures.....	7
6.1 CCTV acquisition.....	7
6.2 CCTV maintenance.....	8
6.3 User access and security.....	8
6.4 Access by Ethical Standards Unit .....	9
6.5 Training and education .....	9
6.6 Ethical use of CCTV systems and recorded material .....	9
6.7 Confidentiality.....	9
6.8 Complaints regarding the CCTV system and its operation.....	10
6.9 Breaches and disciplinary matters .....	10
6.10 Access to CCTV images .....	11
6.10.1 Right to Information and Information Privacy .....	11
6.10.2 CCTV not owned by DJAG.....	11
6.10.3 De-identifying CCTV images.....	11
6.10.4 CCTV at Queensland Courts and Tribunals.....	12
6.10.5 Law enforcement purposes .....	12
6.11 Storage and disposal of surveillance images.....	13
6.12 CCTV signage.....	13
6.13 Ongoing monitoring and assessment.....	13
7. Further information .....	13
8. Definitions.....	14
9. Authority .....	15

<b>10. Related documents.....</b>	<b>15</b>
<b>11. Acknowledgements.....</b>	<b>15</b>
<b>Appendix A: QPS Information Request.....</b>	<b>16</b>
<b>Appendix B: CCTV Signage.....</b>	<b>17</b>

## 1. Purpose

This policy sets out a broad framework for the management of mobile and fixed Closed-Circuit Television (CCTV) cameras and CCTV recording devices and associated data at various Department of Justice and Attorney-General (DJAG) locations.

## 2. Policy Statement

DJAG is committed to protecting its wide range of assets, and to the safety and wellbeing of its staff and members of the public and uses CCTV recording devices for these purposes.

DJAG also uses images from CCTV recording devices to investigate and prevent crime, corrupt conduct, misconduct and breaches of the *Code of Conduct for the Queensland Public Service* and for disciplinary and prosecution purposes.

This policy provides information in relation to the procurement, operation and management of CCTV recording devices and associated images within DJAG. In operating CCTV, DJAG will capture personal information in a range of formats. DJAG will ensure compliance with the *Information Privacy Act 2009* (IP Act) (including the Information Privacy Principles) and the *Right to Information Act 2009* (RTI Act), such as how that personal information is collected, stored, accessed, used, or disclosed and subsequently disposed of.

This policy will generally be sufficient for the needs of all business units. However, where it does not cover individual business unit needs, a local CCTV policy should be developed to address any specific requirements. Business units can contact RTI and Privacy for assistance and further guidance on whether a CCTV policy needs to be developed.

Please note, this policy **does not** cover devices which record audio. This includes devices which capture audio and images at the same time. The *Invasion of Privacy Act 1971* prohibits the recording of private conversations with some exceptions, such as where one party to the conversation consents to the recording.

Where a business unit makes use of these types of devices, a policy addressing the procurement, operation, and management of those devices and, the use or disclosure of any associated images and audio must be developed. Where business units are intending to use surveillance devices which capture audio they should seek legal advice from Legal Advice and Advocacy in the first instance about the legal implications of using this technology.

## 3. Principles

This policy sets out the principles of the operation of CCTV systems across DJAG. CCTV systems will be:

- operated in accordance with Australian legislative requirements and applicable laws;
- operated in a manner that considers privacy implications and the rights of members of the public and public entities;
- operated in a manner which considers human rights, where appropriate; and
- maintained and monitored in accordance with this policy.

All business units have a responsibility to be aware of, and ensure that they are complying with the relevant legislation where CCTV recording devices are deployed. Further information on legislation and information management requirements which apply are located at section 10 – Related documents.

## **4. Application**

This policy applies to all permanent and temporary employees of DJAG, as well as contractors, subcontractors, employment agency staff, clients and work experience students and volunteers (who are defined as workers in the *Work Health and Safety Act 2011*) while working for DJAG.

## **5. Identifying CCTV system ownership**

### **5.1 Usage and ownership**

CCTV systems in use across DJAG are not all owned by the same entity and are subject to different usage controls. This is due to the broad and varied nature of DJAG's work and responsibilities. DJAG maintains agreements with Building Policy and Asset Management (BPAM) at the Department of Energy and Public Works (DEPW) for the procurement and maintenance of CCTV recording devices operated within DJAG. Further information on procurement is outlined at paragraph 6.1.

CCTV recording devices operate in a range of DJAG facilities. DJAG business units may share responsibility for these CCTV recording devices depending on each business unit's purpose for use.

Information on the location of CCTV recording devices operating across DJAG is available from Facilities Services. This list is also available on the [Queensland Government Open Data Portal](#).

### **5.2 Co-location**

CCTV systems in buildings co-located with another entity must be managed in accordance with this policy when the CCTV system is owned by DJAG. Where DJAG CCTV systems inadvertently capture images of other premises, or of individuals who are not accessing DJAG buildings or services, signage should be displayed to indicate that CCTV recording is in operation and individuals' images may be recorded.

DJAG business units in co-located buildings should have their own co-located CCTV policy – a local policy. Such policies should be developed in consultation with other co-located entities and complementary with this policy where applicable. RTI and Privacy is available to assist and provide support and guidance on these policies to relevant business units. The local policy should be specific and relevant to the management and monitoring of CCTV and as such, does not need to be as extensive as this policy.

## **6. Procedures**

### **6.1 CCTV acquisition**

As previously stated, DJAG procures CCTV systems through BPAM, which complies with the DEPW's procurement policies and procedures. If a business unit has assessed a need for the procurement of CCTV systems, normal business processes must be followed. These may include developing a business case for the purchase of the required equipment.

Facilities Services, DJAG will assess the request in collaboration with the business unit to ensure the appropriate CCTV recording device/s are purchased so business needs are met.

Please contact Facilities Services by email at [facilities.services@justice.qld.gov.au](mailto:facilities.services@justice.qld.gov.au) if you are unsure of your business processes or for further guidance on developing a business case for CCTV equipment.

A contracted security specialist may undertake a risk assessment regarding CCTV camera placement. Facilities Services uses the information from the risk assessment to provide recommendations back to the business units outlining whether CCTV would be appropriate. A combination of fixed and mobile CCTV recording devices may be identified and selected for different fields of view as required by business units.

Agreements made between DJAG and BPAM will ensure that contractors hold and maintain appropriate qualifications and licences. Further, agreements should include provisions to ensure that contracted service providers manage footage in accordance with this policy, as well as any individual business unit or local policy, if applicable, and that contractors will be bound by the provisions of the IP Act, as set out in Part 4, and other relevant legislation where appropriate.

## **6.2 CCTV maintenance**

DJAG will ensure that agreements with BPAM include provisions for maintenance, as per usual practice. Facilities Services is responsible for negotiating agreements with BPAM and for ensuring compliance with conditions. These agreements will outline a maintenance regime for CCTV recording devices which will ensure that:

- CCTV recording devices are in full working order;
- clear, recorded vision from each camera is always available with records of down times; and
- log books, detailing maintenance undertaken, are completed.

Business units will regularly monitor and appraise the performance of the CCTV environment to ensure its proper management and operation. Business units are responsible for monitoring and removing obstructions and reporting faults to Facilities Services so that those issues can be rectified via internal processes.

Please report all maintenance matters whether they be related to periodic monitoring or an unexpected issue to Facilities Services by email at [facilities.services@justice.qld.gov.au](mailto:facilities.services@justice.qld.gov.au).

## **6.3 User access and security**

User access to CCTV systems by officers and individuals working for or on behalf of DJAG will be monitored by the relevant business unit. Requests for a change of officer access to the CCTV systems must be sought from the relevant Director within each business unit who is responsible for the CCTV recording devices in use. This includes new officers to DJAG whose roles require them to have access to DJAG CCTV systems. All CCTV monitoring software must be secured, with access to be controlled by role-based authorisation.

Some DJAG facilities may contain control rooms to allow real time monitoring. Officers must have authorisation as part of their role to access these control rooms and CCTV software.



## 6.4 Access by Ethical Standards Unit

DJAG's Ethical Standards Unit (ESU) may require access to images from CCTV systems as part of its investigation processes.

The Executive Director, ESU is authorised by the Director-General to access such material for use as necessary in dealing with alleged corrupt conduct, misconduct and breaches of the *Code of Conduct for the Queensland Public Service*. CCTV images may also be relied upon by the Director-General (or delegates) in disciplinary matters and for the purpose of taking management action against staff.

It may be necessary and appropriate for the ESU to deviate from the protocols outlined in this policy in exceptional circumstances for the purposes of such investigations, and where other legislative requirements may apply.

## 6.5 Training and education

Business units must ensure officers are aware of their obligations under the *Public Service Act 2008*, the *Code of Conduct for the Queensland Public Service* and this policy when using CCTV systems as part of their role.

Any vendors responsible for CCTV within DJAG facilities will provide training to DJAG officers on the operation of the relevant CCTV system and may be engaged to train new authorised officers operating the system as required by their role descriptions.

## 6.6 Ethical use of CCTV systems and recorded material

DJAG has the highest expectation of all officers authorised to use CCTV as part of their role to:

- at all times, act in an honest and lawful manner that is consistent with the protection of human rights and in compliance with the RTI Act, the IP Act, the [Code of Conduct for the Queensland Public Service](#) as well as the *Workplace Policy for the Department of Justice and Attorney-General* ([DJAG's Workplace Policy](#)) when collecting, storing, accessing, using, disclosing or disposing of information in the agency's possession or control in relation to the CCTV system;
- treat all live and recorded images in an ethical manner and with the utmost of care, respect and dignity; and
- interact with all stakeholders in a timely, courteous and cooperative manner.

## 6.7 Confidentiality

Subject to section 6.4, DJAG expects authorised officers to ensure confidentiality of information (that is either in physical possession or within legal control) gathered by or from CCTV operations, by not disclosing or discussing any events with unauthorised personnel or associates who have no direct responsibility relating to CCTV operations.

In addition, authorised officers must not identify any involved person or party with family, friends or acquaintances and must not disclose any information to third parties, including the media, without prior approval in accordance with the policies. Please refer to DJAG's Media Policies and the general provision in the [Public Service Code of Conduct \(1.3 Contribute to public discussion in an appropriate manner\)](#) for further information and guidance.

## 6.8 Complaints regarding the CCTV system and its operation

Complaints received from clients are handled in accordance with DJAG's [Client Complaint Management Policy](#). Internal complaints made by DJAG officers generally will be handled in accordance with the [Individual Employee Grievances \(Directive 11/20\)](#) and the Individual Employee Grievances Policy and Procedure. If a DJAG officer makes a complaint as a client of the department, the complaint will be handled in accordance with the Client Complaint Management Policy.

If DJAG receives a complaint alleging a breach of privacy under the IP Act, it will be managed by RTI and Privacy, which may refer complaints regarding DJAG officers and their use of CCTV recording devices to ESU.

## 6.9 Breaches and disciplinary matters

Business units should have operational specific preventative measures in place to prevent the occurrence of unauthorised use of CCTV recording devices. For example, an audit log can be used to detect possible unauthorised access, disclosure or misuse<sup>1</sup>.

Unauthorised access, disclosure or misuse of CCTV systems and images by an officer of DJAG may be a breach of the [Code of Conduct for the Queensland Public Service](#), the *Public Service Act 2008* and [DJAG's Workplace Policy](#). ESU may decide to investigate alleged breaches of the *Code of Conduct for the Queensland Public Service*, the *Public Service Act 2008*, and DJAG's Workplace Policy.

CCTV images may be used in relation to disciplinary matters and for the purpose of taking management action in respect of public service employees. If a breach is substantiated, disciplinary action may be initiated by a delegated decision maker.

Alleged breaches may also be referred to the Queensland Police Service (QPS), Crime and Corruption Commission (CCC) or another entity where relevant.

DJAG business units are to ensure that staff are aware of:

- the existence and location of CCTV recording devices in and around their workplace;
- the potential for CCTV images to be used in relation to a disciplinary matter or for the purpose of taking management action against staff; and
- this policy.

If a contracted service provider acts contrary to this policy, any local policy and legislative obligations and requirements (outlined at section 6.11), any alleged or confirmed misuse of CCTV images will be managed in accordance with the relevant contract or service level agreement, or referrals made to a law enforcement agency if appropriate.

All authorised officers under any CCTV policy in DJAG will be made aware that recordings are subject to routine and targeted internal or external audits. As such, officers may be required to justify their actions, such as interest in particular CCTV images if necessary.

---

<sup>1</sup> [https://www.oic.qld.gov.au/\\_data/assets/pdf\\_file/0014/41117/report-compliance-audit-bundaberg-regional-council.pdf](https://www.oic.qld.gov.au/_data/assets/pdf_file/0014/41117/report-compliance-audit-bundaberg-regional-council.pdf)

## **6.10 Access to CCTV images**

If access to CCTV images is provided for an authorised purpose, whether the CCTV device is owned by DJAG or another party, a record (for example, in an audit log) is to be created by the officer processing the request, indicating the reason why the CCTV image was extracted to satisfy that it was reasonably necessary, as well as the name of the requestor, the date and time.

Two copies of the original images must be created in an appropriate format and contain information about the images, including the creation date and time stamp, and a methodology of verification:

- one copy is to be made available for the authorised purpose; and
- a second copy is to be retained by the business unit in accordance with the appropriate retention and disposal schedule.

Note: If an incident occurs in an area with CCTV coverage, the relevant business manager should review/request access to any footage that may show the incident to decide whether the footage needs to be retained for future use (such as to assist a police investigation or workers compensation). For further information on incident management refer to the Health, Safety and Wellbeing page on the DJAG intranet.

Further information on access to CCTV images for authorised purposes is provided below.

### **6.10.1 Right to Information and Information Privacy**

Individuals can make a request to access CCTV images under the relevant provisions of the RTI Act and the IP Act. Once a request is received by RTI and Privacy, it will be processed in line with the relevant legislation and statutory time frames. Further information on access under the RTI and IP Acts is available at [www.rti.qld.gov.au](http://www.rti.qld.gov.au). CCTV images may be disclosed to other agencies or organisations in accordance with this policy or where authorised or required by law. Section 6.10.5 provides further information about the disclosure of personal information for law enforcement purposes.

In most instances, a request for access to CCTV images under the RTI or IP Act is received by RTI and Privacy. If such a request is received by another business unit, the request should be forwarded to RTI and Privacy as soon as possible. RTI and Privacy will then contact the relevant business unit to request a copy of the images.

### **6.10.2 CCTV not owned by DJAG**

When the business unit receives a request for CCTV images recorded in DJAG occupied facilities and the CCTV recording device is not owned by DJAG, the request must be forwarded to RTI and Privacy for assessment of authorised purpose. If the request is approved by RTI and Privacy, the request must then be forwarded to Facilities Services.

Facilities Services will submit a written request to the relevant Lease Manager at DEPW who will identify the CCTV system ownership and formally seek the release of images to DJAG.

### **6.10.3 De-identifying CCTV images**

Depending on the type of information requested, CCTV images of other individuals may be de-identified before being released by DJAG.

Where a request for information is made under the RTI or IP Acts and the intention is to disclose that information, if the individuals are not able to be de-identified, reasonable steps will be taken by RTI and Privacy to consult the affected third parties in line with legislative requirements.

#### **6.10.4 CCTV at Queensland Courts and Tribunals**

CCTV is in operation at Queensland Courts and the Queensland Civil and Administrative Tribunal (QCAT). Information is collected for the safety of individuals accessing the courts and QCAT as well as to investigate and prevent crime, corrupt conduct, misconduct and breaches of the *Code of Conduct for the Queensland Public Service* and for prosecution and disciplinary purposes.

The Queensland Courts CCTV policy and procedure outlines requirements for access to information captured by CCTV. Information regarding the use of CCTV at QCAT is located on their [website](#).

#### **6.10.5 Law enforcement purposes**

Copies of CCTV images accessed for law enforcement purposes may be used as evidence in court. If requested, advice should be sought from the relevant law enforcement agency about the proper management of this potential evidence.

Where a disclosure for a law enforcement purpose occurs, under IPP 11(2), a note must be placed on the file indicating that CCTV images have been copied and disclosed for a law enforcement purpose.

Where CCTV images are required by the Queensland Police Service (QPS), the appropriate QPS [Information Request form](#) (Appendix A) may be completed by QPS and submitted to DJAG to action. This form is available on both the DJAG intranet and the QPS intranet and should be submitted to RTI and Privacy ([privacy@justice.qld.gov.au](mailto:privacy@justice.qld.gov.au)) to be processed. However, the request can be received and processed by any business unit. The QPS Information Release form is not mandatory. Accordingly, requests for CCTV images may also be received by letter.

Under IPP 11(1)(e), any business unit processing a request from QPS must satisfy themselves that the disclosure is necessary for one or more of the following by or for a law enforcement agency:

- (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;
- (ii) the enforcement of laws relating to the confiscation of the proceeds of a crime;
- (iii) the protection of public revenue;
- (iv) the prevention, detection, investigation or remedying of seriously improper conduct;
- (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Where a business unit receives a request for CCTV images for law enforcement purposes, and officers are unsure how to process the request, please contact RTI and Privacy for further information on [privacy@justice.qld.gov.au](mailto:privacy@justice.qld.gov.au) or phone (07) 3738 9898.

There are also other mechanisms to access this information such as through warrants and subpoenas. If you are unsure about how to respond to a warrant or subpoena, please seek legal advice from Legal Advice and Advocacy by calling (07) 3738 9521 or by email at [legal.services@justice.qld.gov.au](mailto:legal.services@justice.qld.gov.au).

### **6.11 Storage and disposal of surveillance images**

Original surveillance images are stored for a period of 30 days unless otherwise specified or authorised by a relevant disposal authority under the General Retention and Disposal Schedule (GRDS), another relevant retention and disposal schedule of a business unit as approved by the Queensland State Archivist, by law, or unless directed by the Director-General. Images are then overwritten with new CCTV images.

The retention period covering specific CCTV images which have been extracted and saved for a permitted purpose depends on the circumstances captured by the CCTV system.

The retention period for CCTV images may be different or change depending on the purpose for which the CCTV images were extracted.

Further information on the storage and disposal of surveillance images is available from [Queensland State Archives](#) or contact the relevant local records manager.

### **6.12 CCTV signage**

Reasonable steps must be taken to ensure individuals are aware of the purpose (and legislative authority, if any) for collecting personal information and any entities to which the agency usually discloses information of that kind.

- all business units within DJAG must ensure that appropriate signage is displayed and visible where CCTV cameras are used. CCTV signage must outline the purpose for the collection of personal information via CCTV;
- inform the public of any authority or law which authorises or requires the collection of personal information;
- advise whether it is usual practice to disclose personal information to any entity, the name of that entity and whether the personal information is normally passed on to a second entity;
- identify the owner or controller of the CCTV system in use; and
- inform the public of their right to access the information under the IP and RTI Acts.

An example of CCTV signage is available by emailing [privacy@justice.qld.gov.au](mailto:privacy@justice.qld.gov.au). Refer to Appendix B.

### **6.13 Ongoing monitoring and assessment**

DJAG business units each hold responsibility to regularly monitor, assess and review the performance of the CCTV environment to ensure its proper management and operation. Any identified faults or issues should be managed in accordance with the relevant agreements as outlined in section 6.2, CCTV maintenance.

## **7. Further information**

The following documents are relevant to the application of this policy:

- [CCTV signage \(refer to Appendix B\)](#)

- [Code of Conduct for the Queensland Public Service](#)
- DJAG [CCTV Dataset](#)
- DJAG CCTV Policy
- DJAG's [Client Complaint Management Policy](#)
- [DJAG's Workplace Policy](#)
- [General Retention and Disposal Schedule \(GRDS\)](#)
- [Individual Employee Grievances \(Directive 11/20\)](#)
- Individual Employee Grievances Policy and Procedure
- [Office of the Information Commissioner Camera Surveillance and Privacy Information](#)
- QCAT [website](#)
- [Queensland Courts CCTV Policy](#)
- [Queensland State Archives](#)
- QPS [Information Request form](#)

## 8. Definitions

Term	Definition/ Explanation/ Details
Activities	Workplace operations, processes or functions for the safe and effective delivery of services.
Authorised officer	An authorised officer is an individual working for DJAG who is authorised by virtue of their role to view, operate and perform CCTV related duties as part of their employment. This is determined by the relevant business unit.
Building Policy and Asset Management (BPAM)	Building Policy and Asset Management falls under the Department of Energy and Public Works (DEPW). DEPW manage the procurement and contract management of CCTV systems within DJAG.
Closed Circuit Television (CCTV)	A closed and self-contained television system comprising of cameras, recorders and displays. Signals are not circulated publicly but are monitored and recorded internally.
CCTV images	Images recorded by the CCTV system.
CCTV operations	All aspects of CCTV management, use, recording, maintenance and access to recorded material.
Department of Justice and Attorney-General (DJAG)	Refers to the Department of Justice and Attorney-General Queensland.
Ethical Standards Unit (ESU)	ESU is responsible for the development and implementation of an ethics awareness strategy for DJAG and to foster a culture of integrity and accountability.
General Retention and Disposal Schedule (GRDS)	The GRDS covers records of common activities and functions, transitory, and short term records created as part of routine transactional business practices.
Original images	Unaltered, unedited images. The image data must remain exact to the original recording.
Queensland Police Service (QPS)	QPS works with members of the community to prevent and detect crime, and to make Queensland safer.
Right to Information and Privacy (RTI and Privacy)	RTI and Privacy is responsible for administering DJAG's obligations under the <i>Right to Information Act 2009</i> and the <i>Information Privacy Act 2009</i> .
Security specialist	An individual or organisation contracted to provide advice regarding CCTV and security.
Security	The preparation, protection and preservation of people, property, and information.

## **9. Authority**

*Information Privacy Act 2009*

## **10. Related documents**

Queensland State Archives Managing Closed Circuit Television (CCTV) Records, Guideline for Queensland Public Authorities

Standards Australia CCTV standard AS 4806.1-2006:

- AS 4806.1-2006- Closed Circuit Television (CCTV) – Part 1: Management and operation
- AS 4806.2-2006- Closed Circuit Television (CCTV) – Part 2: Application Guidelines
- AS 4806.3-2006- Closed Circuit Television (CCTV) – Part 3: PAL signal timings and levels
- AS 4806.4-2006- Closed Circuit Television (CCTV) – Part 4: Remote video
- AS 2201.1:2007 – Intruder alarms systems – Client’s premises – Design, installation, commissioning and maintenance
- AS/CA S009:2013 – Installation requirements for customer cabling (Wiring Rules)

*Crime and Corruption Act 2001*

*Crime and Corruption Amendment Act 2016*

*Information Privacy Act 2009*

Information Standard 18: Information Security

Information Standard 31: Retention and Disposal of Public Records

*Public Records Act 2002*

*Public Service Act 2008 (until repealed)*

*Public Sector Act 2022 (upon commencement)*

Records Governance Policy

*Right to Information Act 2009*

*Security Providers Act 1993*

*State Buildings Protective Security Act 1983*

*Work Health and Safety Act 2011*

*Human Rights Act 2019*

## **11. Acknowledgements**

The Office of the Queensland Ombudsman’s CCTV Policy structure meaningfully assisted in the creation of this document. Content about CCTV available from the Office of the Information Commissioner website was used to create this document.

## Appendix A: QPS Information Request

Department of Justice and Attorney-General

www.justice.qld.gov.au

### Queensland Police Service Information Request

#### Requesting officer

Name		Rank	
Registered No.		Region	
District		Station	
Email		Phone	Fax
"I certify that this information is reasonably necessary pursuant to Principle 11(1) of the <i>Information Privacy Act 2009</i> ".			
Requesting officer signature		Date	

#### Commissioned officer authorisation

Name		Rank	
Registered No.		Region	
District		Station	
"I am satisfied this information is reasonably necessary pursuant to Principle 11(1) of the <i>Information Privacy Act 2009</i> ".			
Commissioned officer signature		Date	

#### Reason for request and details of offence

Reason for request, including what is being investigated.			
Location			
Details of the offence			
Date	Time	QPRIME Occurrence No.	

#### Details of why the information is necessary for the investigation.

Details of any law requiring or authorising the Department of Justice and Attorney-General (DJAG) to provide the information.	
---	--

**Send to:** Right to Information and Privacy, GPO Box 149, BRISBANE QLD 4001. **Phone:** (07) 3738 9893

**Email:** RTIAdministration@justice.qld.gov.au

#### Internal use only

Date request received by DJAG	/ /	Receiving officer	
-------------------------------	-----	-------------------	--

The Department of Justice and Attorney-General must not disclose personal information unless an exception in paragraphs (a) to (f) of the IPP 11(1) of the *Information Privacy Act 2009* (Qld) applies. The Department of Justice and Attorney-General will assess on a case-by-case basis whether an exception applies. The Department of Justice and Attorney-General may disclose information, if it is satisfied on reasonable grounds that the disclosure of information is necessary for one or more of the paragraphs in IPP 11(1)(e)(i) to (v).

jag\_18\_05\_2020 RTI 6439



Queensland Government



## Appendix B: CCTV Signage

# ATTENTION

## CCTV Cameras in operation



The Department of Justice and Attorney-General is collecting your personal information on a closed circuit television system (CCTV) in and around this building. The personal information collected is being used for the purposes of public safety, crime prevention and detection.

Your personal information will only be accessed by persons who have been authorised to do so.

This information may be provided to the Queensland Police Service for law enforcement purposes. Your information will not be given to any other person or agency unless required by law. Your personal information is handled in accordance with the Information Privacy Act 2009.

**For further information, please refer to the Department of Justice and Attorney-General's Right to information and Privacy page at [www.justice.qld.gov.au](http://www.justice.qld.gov.au)**