CCTV Electronic Surveillance Policy

1. Purpose

The purpose of this policy is to establish a clear framework for the responsible, lawful and ethical use of Closed-Circuit Television (CCTV) systems at Toowoomba Anglican School (TAS). The School recognises that CCTV involves the collection of personal information and therefore must be managed in a way that respects privacy, maintains trust and complies with legal obligations.

CCTV is not intended to replace supervision or duty of care, nor is it to be used for routine monitoring of staff or students.

The School's CCTV systems do not record audio.

2. Scope

This Policy applies to all CCTV systems owned, operated, or managed by the School, including all associated equipment, software, and storage systems. It also applies to all individuals who may be captured by CCTV, including Students, Staff, Contractors, Volunteers, and Visitors.

The Policy governs the full lifecycle of CCTV data, including the collection, use, storage, access, disclosure, and disposal of recorded footage. It also outlines the responsibilities of staff involved in managing or accessing CCTV systems.

3. Policy Statement

The use of CCTV systems within Toowoomba Anglican School is intended to:

- Support the safety and well-being of the school community
- Deter and assist in the investigation of anti-social behaviour and potential criminal activity
- Provide objective evidence for incident investigations, including any child protection matters
- Monitor and protect School assets

CCTV is not intended to create an environment of constant surveillance or supervision.

4. Principles

The School adopts principles consistent with the Information Privacy Act 2009 (Qld) as best practice and is guided by the principles of safety, proportionality, transparency, and legal compliance. Surveillance will only be used where there is a legitimate purpose and will not intrude unreasonably into personal privacy.

TAS is committed to managing all footage in accordance with all relevant Commonwealth and Queensland legislation relating to privacy, surveillance and safety. The School's Privacy Policy

supports this commitment and details how personal and private information is collected, use and retained.

4.1. Information Collection and Use

The School will take all reasonable actions to ensure that:

- CCTV footage is taken and personal information recorded is limited to what is reasonably necessary for the intended uses of the CCTV
- Individuals are made aware of CCTV use through appropriate signage and communications
- CCTV coverage shall not be unreasonably intrusive or installed in areas where individuals have a reasonable or high expectation of privacy
- CCTV footage is only used for its intended purposes unless an exception applies, an individual's express permission is supplied or the School is directed by an authorised or legal authority
- Steps are taken to protect CCTV data from misuse, interference, loss or unauthorised access
- Individuals may request access to their personal information where appropriate and in adherence with the Australian Privacy principles.

CCTV footage may be used in employment-related investigations only where it is directly relevant to a specific incident and consistent with procedural fairness.

While the CCTV system is primarily in place to keep everyone safe and secure, the School recognises that it may occasionally capture positive moments or examples of exemplary student behaviour that celebrate our school values. In these cases, we may wish to share these highlights with our school community. However, footage or images will only ever be shared with the prior written consent of everyone identifiable in the footage (or their Parents/Guardians in the case of students).

Consent is always voluntary, and individuals and families have the right to decline or withdraw their permission at any time without needing to provide a reason.

4.2 Camera Locations

CCTV cameras may be installed in locations that have been risk assessed as requiring surveillance to monitor safety or security risks. This may include high-traffic, isolated or vulnerable areas, or areas where incidents have occurred.

Common locations may include:

- **Access points:** School entrances or exits
- **Building interiors**: such as reception areas, public access areas or isolated areas
- **Outdoor areas:** External play spaces, car parks, school ovals, aquatic centre, locations removed from main School Close

- **Areas monitored to support Child Safety:** Inside School vehicles and busses, as approved by the Principal.
- **Targeted Areas:** Area identified through risk assessment or incident as being vulnerable to vandalism or break in

Prohibited Areas Include:

- **Hygiene and Change Areas:** Toilets, bathrooms, shower/bathing facilities, Aquatic Centre change facilities
- **Boarding Areas:** Bedrooms, dormitories, areas where students have a reasonable expectation of privacy. CCTV in boarding environments will only be used in shared/common areas for safety and security and does not replace active supervision.
- **Health Care and Support:** Health Centre interiors and Counselling areas

The placement of cameras will be determined through a risk-based approach that considers the nature of the environment, the level of risk and the potential impacts on privacy. The School may undertake a Privacy Impact Assessment (PIA) as part of the risk assessment phase prior to the installation of new cameras.

Cameras must not be installed in areas where people have a reasonable expectation of privacy.

4.3. Notification and Transparency

The School will be transparent with its use of CCTV monitoring.

- **Signage:** Clearly visible signs will be placed in monitored areas, and the general school grounds indicating the use of CCTV cameras monitoring.
- **Notice:** Reasonable communications and notice of CCTV monitoring will be provided to the school community through relevant communication channels and documentation.
- **Website:** The School will include this policy on the School's Website in the "Policy" section.

5. Data Management

Data collected will be handled in accordance with the Schools Privacy Policy and relevant Privacy legislation.

5.1. Access and Storage

Access to Live or recorded footage is strictly limited to designated and authorised senior staff whose professional responsibilities directly align with the defined safety and security purposes or management of the system.

Authorised personnel must limit their access to only that which is relevant and appropriate for their specific role and authority. Access may only occur when it is necessary to support the health, safety, and wellbeing of the School community or infrastructure, or to comply with legal and internal/external investigative requirements.

CCTV recordings are maintained as part of the School's secure digital network environment. As such, the School and its network providers will take all reasonable steps to protect against loss, unauthorised access, use or misuse.

5.2. Use and disclosure

Disclosure of footage may occur where:

- It is required or authorised by law;
- It is requested by an authorised or legal authority e.g. Queensland Police Service;
- It is necessary to prevent or lessen a threat to the safety of any person;
- It is approved by the Principal or their delegate for a legitimate School purpose, and in accordance with the School Privacy Policy and relevant legislation.

CCTV footage must not:

- Be used for entertainment or personal purposes;
- Be used for staff performance monitoring;
- Be shared via personal (non-work) devices or unsecured platforms;
- Be used for commercial purposes.

Any decision to disclose CCTV footage to a third party under this section, will be documented in a Disclosure Log. Advice is to be sought from the Schools Privacy Officer before any footage is released.

5.3. Individual Access Request

Individuals may request access to CCTV footage that contains their personal information.

Requests must be:

- Be made in writing to the Principal or their delegate
- Clearly identify the relevant timeframe and location
- Clearly articulate the reason for the request

Access may be refused where:

- It would have an unreasonable impact on the privacy of other individuals
- The footage cannot be reasonably de-identified, or
- The request does not meet legislative requirements.

All requests will be handled in accordance with applicable privacy legislation.

5.4. Retention

CCTV footage is generally kept for 30 days after recording. Footage required for incident review or investigation may be retained for the duration of that investigation or any related legal process, if necessary. If a request for CCTV footage is received from an authorised authority

after the expiration of the 30-day retention period, the School will, where practicable and subject to resource constraints, take reasonable steps to identify and recover any footage that may still be available.

The School cannot guarantee the availability of footage beyond the stated retention period.

This retention period reflects a balance between operational needs and privacy minimisation obligations.

5.5. Data Breach Management

CCTV footage is treated as personal information. In the event of a suspected or actual data breach:

- The incident must be reported immediately to the Principal and Privacy Officer;
- Access to affected systems will be reviewed and restricted as appropriate,
- An investigation into the breach will be undertaken, and
- Appropriate remedial actions will be implemented.

Where required, the School will comply with the Notifiable Data Breaches (NDB) Scheme, including notification to affected individuals and the Office of the Australian Information Commissioner.

5.6 Complaints and Queries

Complaints regarding the use of CCTV surveillance should be made in writing to the School Principal.

Queries about this policy may be made in writing to the School Privacy Officer at privacyofficer@taschool.qld.edu.au

6. Responsibilities

Persons	Responsibilities
Principal	• Provides oversight of governance and policy compliance • Ensure appropriate resources are available to meet compliance with this policy • Make decisions on access requests in line with the School Privacy Policy and relevant legislation
Authorised Staff (with access to CCTV)	• Comply with this policy • Ensure that footage is only used for the purpose for which it was intended e.g. primary purpose unless written permission is given by individuals • Ensure that footage is not shared with unauthorised persons, misused, lost or accessed by unauthorised persons
All Staff	• Comply with this policy
Privacy Officer	• Provide advice to the Principal or their delegate regarding the School's privacy responsibilities • Maintain the School Disclosure Log

	• Contribute to Privacy Impact Assessments (PIAs) for new or modified CCTV systems • Work in conjunction with the Principal and authorised staff to ensure that CCTV systems are operated in a manner that is lawful, transparent, and respectful of individual privacy.

7. Related Policies and Procedures

This Policy should be read in conjunction with the following School policies:

- *Privacy Policy*
- *Child Safe Policy*
- *Work Health and Safety Policy*

8. Relevant Legislation

- *Privacy Act 1988 (Cth)*
- *Information Privacy Act 2009 (Qld)*
- *Right to Information Act 2009 (Qld)*
- *Work Health and Safety Act 2011 (Qld)*
- *Child Safe Organisations Act 2024 (Qld)*

9. Definitions

Term	Definition
Access request	A formal request to view or obtain CCTV footage, including requests made under applicable privacy legislation
Authorised Personnel	Staff members who have been formally approved by the Principal (or delegate) to access, manage, or review CCTV systems or footage as part of their role and responsibilities.
CCTV (Closed Circuit Television)	A system of cameras and associated equipment used to monitor and/or record visual images of activities within the School premises for safety, security, and operational purposes.
CCTV footage/recording	Any visual image or video captured, stored, or processed by the School's CCTV system, including both live and recorded data.
Data Breach	Unauthorised access to, disclosure of, or loss of CCTV footage or personal information that may result in serious harm to an individual.
Disclosure	The release, sharing, or provision of CCTV footage or information to any person or organisation outside the authorised access framework, including law enforcement agencies or external parties.
Personal Information	Information or an opinion about an identified individual or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not, as defined under the *Privacy Act 1988 (Cth)*.

Privacy Impact Assessment	A formal process used to identify and assess privacy risks associated with CCTV systems or changes to surveillance practices, and to ensure appropriate controls are implemented.
Reasonable Expectation of Privacy	Circumstances in which an individual would reasonably expect not to be subject to surveillance.

10. Policy Information

Accountable Officer	*Privacy Officer*
Responsible Committee	*Executive*
Policy Framework	*Privacy*
Record Number	*TAS_PRIPOL_02*
Revision Number	*1.0*
Approval Date	*April 2026*
Review Date	*March 2028*

The School reserves the right to update this policy at any time to reflect legislative changes or operational requirements.