



# SURVEILLANCE POLICY

Approved: 12/2025  
Approved By: Board  
Effective: 4/2026  
Next Review: 2028

[www.dominic.tas.edu.au](http://www.dominic.tas.edu.au)

## PURPOSE

Dominic College (the College) is a K-10 Catholic School in the Salesian Tradition. The policies of the College, underpinned by Gospel values, serve to promote the wellbeing, dignity, and uniqueness of each person, and ensure the College meets its duty of care and legal and regulatory obligations.

The Charter for Salesian Schools sets out four central pillars that embody our founder St John Bosco's vision and guides the College in all aspects of school life. Dominic College draws its inspiration from these four pillars and strives to be:

- A **HOME** that welcomes
- A **PARISH** that evangelises
- A **SCHOOL** that prepares for life
- A **PLAYGROUND** where friends meet and enjoy themselves

Closed Circuit Television (CCTV), License Plate Recognition Technology (LPR) and other surveillance systems (the **Surveillance Systems**) are in operation at the College for the safety and security of individuals while they are within the College's property boundary and for the security of the College work site. LPR technology is used to monitor and record vehicle movements on school grounds.

Surveillance Systems provide the ability to monitor and record activities that occur on College grounds and assists in the identification of criminal and/or anti-social behaviour. Cameras will be installed in public areas which include but are not limited to building entrances, hallways; learning spaces; car parks; playground areas; front offices where staff, students, contractors, volunteers, visitors, and parents/carers come and go.

As part of our commitment to ensuring a safe and secure learning environment, cameras are installed in some classrooms and may be placed in other classrooms at the College's discretion. This measure is intended to enhance the safety of our students and staff, deter inappropriate behaviour, and provide a secure atmosphere conducive to learning. The use of Surveillance Systems will be conducted with respect for privacy and in alignment with our Catholic and Salesian values of trust, respect, and dignity for all individuals.

The College believes that the implementation of Surveillance Systems helps to create a safer and more secure environment and as the Surveillance Systems hold imagery of vulnerable people within our care there are high expectations in relation to the implementation, access, and management of these systems.

## SCOPE

This policy applies to all College staff and in particular employees who are responsible for the setup, maintenance and/or management of Surveillance Systems; who access Surveillance Systems to review, retrieve, download or release footage from Surveillance Systems; and who view security footage.

This policy applies during and outside school hours and every day of the calendar year.

## POLICY STATEMENT

This policy establishes the expectations, responsibilities, and requirements for Surveillance Systems at Dominic College. It aims to:

- Enhance the safety and security of students, staff, and visitors while on College grounds.

- Deter and assist in the prevention of criminal and anti-social behaviour on College grounds.
- Provide a secure environment that supports effective teaching and learning.
- Ensure that the use of Surveillance Systems is respectful of privacy and aligns with the College's Catholic and Salesian values of trust, honesty, respect, and dignity.
- Establish clear expectations, responsibilities, and procedures for the access, review, retrieval, release and retention of security footage.
- Comply with relevant legislation and guidelines, ensuring that Surveillance Systems are operated lawfully and ethically.

All persons covered by this policy are required to comply with its provisions, support its aims and contribute to its effective implementation.

## DEFINITIONS

TERM	MEANING
<b>Authorised Users</b>	<ul style="list-style-type: none"> <li>• Principal</li> <li>• Deputy Principals</li> <li>• Chief Financial and Operations Officer</li> <li>• Director of Learning and Wellbeing (Early Primary)</li> <li>• Director of Learning and Wellbeing (Upper Primary)</li> <li>• Director of Learning and Wellbeing (Secondary)</li> <li>• House Lead Teachers: Bosco, Guzman, Savio, Siena</li> <li>• Lead Teachers: Kinder/Prep, Year 1/2, Year 3/4, Year 5/6</li> <li>• E-Learning Manager</li> <li>• Facilities and Projects Manager</li> </ul>
<b>Authorised Viewers</b>	<p>Includes:</p> <ul style="list-style-type: none"> <li>• Authorised Users.</li> <li>• Lead Teacher assisting with an investigation.</li> <li>• Lead Teacher who needs to be aware of an incident in order to support or sanction a student, and/or to communicate with parents and relevant teachers.</li> <li>• Child Safety Officer.</li> <li>• Privacy Officer.</li> </ul>
<b>Animal Husbandry Team</b>	<p>Refers to the team comprising:</p> <ul style="list-style-type: none"> <li>• Lead Teacher (Agriculture and Animal Technologies)</li> <li>• Classroom Teacher formally assigned animal husbandry duties</li> <li>• Learning Support Assistant (Animal Husbandry)</li> </ul>
<b>College Retention Period</b>	<p>Is the maximum period the College will retain security footage as determined by the E-Learning Manager and the Surveillance System parameters. The College reserves the right, at its discretion and in accordance with this policy, to retain footage beyond the College Retention Period, however, the College will not retain footage beyond the College Retention Period if that footage is not required for use by the College.</p>
<b>Real Time Monitoring</b>	<p>Refers to the continuous and instantaneous observation and analysis of live video feeds from CCTV cameras.</p>
<b>School Environment</b>	<p>Is any physical or virtual place made available or authorised by the College for use by children during or outside school hours. This includes:</p> <ul style="list-style-type: none"> <li>• College grounds and facilities.</li> <li>• Online College environments, including email, intranet Systems and social media platforms.</li> </ul>

TERM	MEANING
	<ul style="list-style-type: none"> <li>Other locations provided by the College for a child's use, including locations used for School Activities and School Events.</li> </ul>
<b>School Community</b>	All persons who are associated with Dominic College in some way. This includes workers, coaches, students, parents, guardians, carers, step-parents, relatives, friends, supporters, volunteers and visitors when in any school environment or when attending any school-related function, activity or event.

## SURVEILLANCE SYSTEMS PRINCIPLES

- In accordance with the requirements of the *Listening Devices Act 1991* (Tas) Surveillance Systems in use by Dominic College must not be audio recording whether it be real-time monitoring or background recording.
- Surveillance Systems are implemented to monitor criminal or anti-social behaviour and must be treated as systems which hold sensitive records.
- Access to Surveillance Systems is controlled and authorised in accordance with this policy.
- Access to Surveillance Systems must be for the purpose outlined in this policy and only in accordance with this policy.
- Authorisation to access Surveillance Systems is **not** authorisation to access all areas or all cameras. Access authorisation is only for the specific camera/s covering areas where an incident is alleged to have occurred.
- Security footage cannot be perused for interest's sake or out of curiosity.
- Security footage can only be viewed in accordance with this policy.
- Security footage can only be downloaded, retained and stored in accordance with this policy.
- Security footage can only be released in accordance with this policy.
- The College will not have cameras placed in locations stipulated in this policy.
- Cameras must not be installed with the primary purpose of viewing into adjacent premises buildings, commercial premises, or private residences unless requested by Tasmania Police or the Australian Federal Police.
- Access history to Surveillance Systems must be logged, auditable and documented as per this policy.
- Real-time monitoring must be conducted within the parameters established in this policy.
- The College must have appropriate signage in accordance with this policy.
- The School Community will be made aware of the use of Surveillance Systems through signage or other communication channels.

- Any request to access or view footage will be considered in accordance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles, other legal obligations, this policy, the College's Privacy Policy and any other applicable College policies.
- The College must ensure there is controlled physical access to the Surveillance Systems in accordance with this policy.
- In implementing and managing Surveillance Systems the College must meet the following cybersecurity requirements:
  - be implemented with the principle of least privilege, and
  - be limited in who can view and recover the footage as per this policy, and
  - utilise individually named, non-generic user accounts with granular access permissions, and
  - not be published to or accessible from the Internet without multi-factor authentication (MFA) or other phishing resistant authentication mechanism (e.g. biometric), and
  - provide strong encryption of data (including metadata, authentication and video data) in transit and at rest.

## **AUTHORISED ACCESS**

- Authorised Users have authority to access the Surveillance Systems to review, retrieve and download security footage in accordance with this policy.
- All Authorised Users who access the Surveillance Systems must log the activity using the 'Surveillance System Access Log'. This log entry must be created within one business day of the footage being accessed.
- Authorised Viewers have authority to **view** security footage. Authorised Viewers can only view footage in the presence of an Authorised User.
- Staff who witness, become aware of, or are managing an incident that requires viewing of footage, must discuss this with the relevant Authorised Viewer who will determine if the footage needs to be viewed. Note that if the staff member who witnesses or becomes aware of an incident, or is managing an incident, is not an Authorised Viewer, they will not be able to view the footage.
- ICT contractors and authorised external vendors must obtain approval from the E-Learning Team prior to being granted access to critical systems and services, such as Surveillance Systems. Such ICT contractors and authorised external vendors must sign a non-disclosure agreement prior to being granted access.
- Authorised Users must undertake training with a suitably qualified staff member on this policy and the use of the Surveillance Systems, including best practice for sharing stored footage in alignment with this policy. Training must be undertaken prior to granting access to the Surveillance Systems and must confirm in writing they have read, understand and agree to comply with this policy.

## **Animal Husbandry Access**

- Members of the Animal Husbandry Team have authority to access the Surveillance Systems to review, retrieve, and download security footage in accordance with this policy, however, this authority is restricted to the cameras covering the Animal Husbandry area.

- Members of the Animal Husbandry Team are to use this access solely for the purpose of monitoring the wellbeing of the animals on College grounds and only in accordance with this policy.
- They must log the activity using the 'Surveillance System Access Log'. This log entry must be created within one business day of the footage being accessed.
- Members of the Animal Husbandry Team must undertake training with a suitably qualified staff member on this policy and the use of the Surveillance Systems, including best practice for sharing stored footage in alignment with this policy. Training must be undertaken prior to granting access to the Surveillance Systems and must confirm in writing they have read, understand and agree to comply with this policy.

### E-Learning Team Access

- Members of the E-Learning Team have authority to **access** the Surveillance Systems to undertake health checks of CCTV cameras and recording software in accordance with the E-Learning Maintenance Schedule and this policy, to ensure they are online and recording. Except for the E-Learning Manager, other members of the E-Learning Team do **not** have authority to review, retrieve or download footage.
- These checks are completed by accessing footage that was recorded outside of normal work or school hours and must be entered into the 'Surveillance System Access Log' within one business day of the footage being accessed.
- Members of the E-Learning Team must undertake training with a suitably qualified staff member on this policy and the use of the Surveillance Systems, including best practice for sharing stored footage in alignment with this policy. Training must be undertaken prior to granting access to the Surveillance Systems and must confirm in writing they have read, understand and agree to comply with this policy.

### CAMERA PLACEMENT AND CONFIGURATION

- When installing cameras, the view angle of cameras will be carefully considered to ensure that there is no possible view into the following banned locations either within or in view of:
  - wet areas (toilets, bathrooms, showers)
  - changerooms or dressing rooms
  - breast feeding rooms
  - rooms designated for a specific purpose where there is a reasonable assumption of privacy (e.g. College Counsellors Office)
  - first aid rooms
  - other areas where individual privacy is paramount.
- Placement of cameras should be considered to ensure that their placement is not breaching or infringing on a person's personal privacy. This includes consideration of whether:
  - privacy filters on staff computer monitors and mobile devices reduces the risk of a person's personal privacy being impacted
  - an external camera has a primary viewing angle into a private residence
  - cameras, and other IoT (Internet of Things) devices in use, such as environment sensors, are to be configured to ensure no audio is recorded via the device.

## REAL-TIME MONITORING

- The College reserves the right to have real-time monitoring of Surveillance Systems in key public areas of interest to ensure the safety of all individuals on College grounds.
- User accounts used for real-time monitoring only, must not have access to historic footage.
- In areas where livestock remain on College grounds outside of school hours, real-time monitoring by the Animal Husbandry Team is facilitated in accordance with this policy.
- Careful consideration must be given to the location of any screen or TV used for real-time monitoring taking into consideration the privacy of individuals appearing in the footage. For example, the screen or TV must be out of sight of the general public, parents and students.

## SIGNAGE

- The College will have signage at the primary entry points to the site advising that the site is monitored by Surveillance Systems.
- Signs must be clearly visible, distinctive, and located in areas with good lighting, placed at average eye level and large enough so that any text can be read easily.
- Signs should include a mix of text and symbols.
- Signs should be checked regularly for damage, theft, or vandalism.

## EXTERNAL RELEASE OF FOOTAGE

- Footage will **not be released** to external parties unless required or permitted by law. For the purposes of this policy, an external party is anyone who is not a College employee.
- Any **release** of footage to external parties (including where required by law) must be approved by either the Principal, Deputy Principals, Chief Financial and Operations Officer, College Child Safety Officer or College Privacy Officer, must be in accordance with this policy, and must be downloaded and stored in a secure, College approved location.
- Any security footage approved for **release** must be appropriately redacted so that, where possible, faces of individuals are blurred unless approved otherwise by the Principal, Deputy Principals, Chief Financial and Operations Officer, College Child Safety Officer, or College Privacy Officer, or if instructed by a Court or required by law.
- Any request to **view** footage by external parties will be considered in accordance with our legal obligations, and College policies and procedures.

## ACCESSING, DOWNLOADING AND RELEASING FOOTAGE

### Routine Internal Access to Security Footage

- Each time security footage is accessed from the Surveillance Systems the staff member (Authorised User, E-Learning, Animal Husbandry) must record the activity and provide the details using the 'Surveillance System Access Log' within one business day of the footage being accessed.

- Under no circumstances can security footage (including screenshots) be emailed, shared using links, or distributed by any other means.
- **During the College Retention Period**, security footage can only be viewed by authorised persons using the software platform where the footage is recorded. Footage may be downloaded and stored during the College Retention Period but only in accordance with the 'Retaining Security Footage' Clause in this policy.
- Footage can be downloaded from the software platform and stored in a College approved location, if the footage needs to be retained for use **beyond the College Retention Period** or if explicit approval has been obtained to release it in accordance with this policy.
- Security footage can only be viewed by Authorised Viewers. Staff need to be aware of the physical space used when viewing recordings. This space must be a private space where Non-Authorised Persons are not able to see the footage being viewed.

### Retaining Security Footage

- While undertaking investigations or responses to incidents or events, consideration should be given to the need to download and store footage for retention beyond the College Retention Period including for any actual or potential future legal proceedings, investigations or complaints.
- Any footage which has been viewed by external parties or approved for release to external parties must be retained.
- Any footage downloaded and retained can only be stored in a secure, College approved location, and to which access will be restricted.

### Law Enforcement Request for Security Footage

If the College receives a request for security footage from a law enforcement agency (e.g. Tasmania Police, the Australian Federal Police or other recognised law enforcement agency within the Australian jurisdiction), security footage can be viewed but not released without approval from either the Principal, Deputy Principals, Chief Financial and Operations Officer, College Privacy Officer or College Child Safety Officer. The following actions must also be undertaken:

- Details must be recorded using the 'Surveillance System Access Log'.
- A detailed reason for the download must be provided and documented.
- The case number from the law enforcement agency and the contact person must be documented.
- Security footage must be **securely** delivered using a **secure** method requested by the relevant law enforcement agency and in line with this policy.

## PHYSICAL ACCESS TO THE SYSTEMS

### Restricted Access

Access to the physical Surveillance Systems is strictly limited to designated individuals. This includes authorised security contractors and E-Learning staff responsible for systems maintenance. Unauthorised personnel are prohibited from accessing the physical Surveillance Systems or control room.

## Access Control Measures

To ensure secure access to the surveillance monitoring area or control room, access control measures must be implemented. These controls include locked doors via swipe cards or master locks and restricted access.

## Logging and Auditing

All attempts to access the Surveillance Systems are logged for accountability. The logs include:

- User Details: Identification of the individual accessing the Systems
- Date and Time: Precise timestamp of the access attempt
- Actions Taken: Description of activities performed during access

Regular audits of the access logs will be conducted to ensure compliance with the policy and to identify any unauthorised access attempts.

## RECORD KEEPING

- Access Log Records will be kept for the required length of time in accordance with our legal obligations, College Records Management Policy, and the Records Retention and Disposal Schedule for Non-Government Schools.
- Security footage will be retained by the College for the College Retention Period before it is automatically deleted or overwritten. This Retention Period ensures that the College can effectively monitor and review footage for specified business purposes while respecting privacy and managing storage efficiently.
- The College reserves the right to retain security footage beyond the College Retention Period at its discretion. This includes but is not limited to, footage of an incident that is under internal or external investigation (or may be in the future), is the subject of a complaint (current or potential), or for any potential legal proceedings that may arise in the future.
- Staff must ensure any retained security footage is appropriately named so it is clearly identifiable, and document the reason for downloading, details of who has viewed it and why, and details of any approved external release.

## BREACHES OF THIS POLICY

Any breach of this policy will be assessed on a case-by-case basis, and will consider the severity, intent, frequency and impact of the breach. The College response will be guided by its Catholic and Salesian ethos, its policies and procedures, and any legal or regulatory obligations.

A breach of this policy may result in (but is not limited to) one or more of the following.

- Reminder of our expectations either verbally or in writing.
- Referral to College leadership.
- Corrective actions including retraining, professional development, supervision or performance management.
- Formal warning.
- Removal from specific duties.
- Removal of access to Surveillance Systems.
- Suspension or termination of employment.

- Referral to external authorities where required by law or regulator including Tasmania Police, Office of the Australian Information Commissioner, Teachers Registration Board, Registration to Work with Vulnerable People or other relevant bodies.

## ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
<b>Authorised Users</b>	<ul style="list-style-type: none"> <li>• Familiarise themselves with and comply with this policy.</li> <li>• Authority to access the Surveillance Systems to review, retrieve and download security footage in accordance with this policy.</li> <li>• Ensure policy awareness and compliance by relevant members of their team and ensure appropriate training and support.</li> <li>• Ensure any breaches of this policy are acted upon as soon as reasonably possible.</li> <li>• Report any breaches of this policy to the Principal, Chief Financial and Operations Officer, and College Privacy Officer.</li> <li>• Lead policy implementation and enforcement and support continuous improvement.</li> <li>• Ensure the College has the appropriate resources required to meet its obligations.</li> </ul>
<b>Authorised Viewers</b>	<ul style="list-style-type: none"> <li>• Familiarise themselves with and comply with this policy.</li> <li>• Authority to <b>view</b> security footage in accordance with this policy.</li> </ul>
<b>E-Learning Team</b>	<ul style="list-style-type: none"> <li>• Familiarise themselves with and comply with this policy.</li> <li>• Authorised to <b>access</b> the Surveillance Systems to undertake health checks of cameras and recording software, in accordance with the E-Learning Maintenance Schedule and this policy, to ensure they are online and recording.</li> <li>• Authorised to access the physical Surveillance Systems or control room in accordance with this policy.</li> <li>• Authorised to grant access to the physical Surveillance Systems or control room to authorised security contractors responsible for systems maintenance in accordance with this policy.</li> </ul>
<b>Animal Husbandry Team</b>	<ul style="list-style-type: none"> <li>• Familiarise themselves with and comply with this policy.</li> <li>• Have authority to access the cameras covering the Animal Husbandry area to review, retrieve, and download security footage in accordance with this policy.</li> </ul>
<b>Governance Manager</b>	<ul style="list-style-type: none"> <li>• Oversee the ongoing review of the policy to ensure continuous improvement, and keep abreast of business requirements and regulatory and legislative changes.</li> <li>• Ensure this policy is accessible in the College Policy Library, the College website and upon request.</li> </ul>
<b>Principal/ Deputy Principals/ CFOO/ Child Safety Officer/ Privacy Officer</b>	<ul style="list-style-type: none"> <li>• Familiarise themselves with and comply with this policy.</li> <li>• Approve the release of security footage to external parties (including where required by law).</li> </ul>

## RELATED DOCUMENTS

Related documents include but are not limited to those listed below.

### College Policies and Procedures

- Child Safe Policy
- Privacy Policy
- Records Management Policy
- Staff Code of Conduct

### Legislation

- Child and Youth Safe Organisations Act 2023 (Tas)
- Children, Young Persons and Their Families Act 1997 (Tas)
- Education Act 2016 (Tas)
- Listening Devices Act 1991 (Tas)
- Privacy Act 1988 (Cth) and Australian Privacy Principles

### Other

- Records Retention and Disposal Schedule for Non-Government Schools, 2nd Edition, April 2018 (Australian Society of Archivists)
- Terms, Definitions, Acronyms and Legislation Guide

## LOCATION AND ACCESS

College policies are stored and accessed through designated platforms to ensure the correct information is available to the appropriate audience.

This policy is available in the College Policy Library on SharePoint accessible by all staff. It is also available on the College website or upon request.

Printed copies of this policy are not considered current and should not be relied upon. Always refer to the SharePoint version or the Website version for the current, approved policy.

## FURTHER INFORMATION

If you would like further information about the way the College manages its Surveillance Systems, please contact the College Privacy Officer by email at [privacy@dominic.tas.edu.au](mailto:privacy@dominic.tas.edu.au)