CCTV AND VAPE DETECTION PROCEDURE

CONTEXT STATEMENT

St Mark's College (College) is committed to providing safe environments for all employees, students and visitors. Closed Circuit Television (CCTV) and Vape Detection systems are security and safety measures that the College can use to support a safe and secure environment. The College recognises the need to ensure a balance between the individual's rights to be free from invasion of privacy and the duty to promote a safe environment for all employees, students and visitors, and the protection of property.

This procedure has been developed as required under the SACCS CCTV Video Surveillance Policy to regulate access to content created using surveillance. This procedure aligns with the SACCS policy to which the College is bound.

PURPOSE

This policy outlines the requirements relating to the implementation, installation and responsible management and use of CCTV and Vape Detection at the College.

The purpose of this policy is to enhance the security of property owned and operated by the College and provide all employees, students and visitors with a safe environment in which they can work and study.

Installing CCTV systems and Vape Detection on college grounds can support the College by:

- acting as a deterrent and reducing the likelihood of vandalism and theft on college grounds,
- deterring misconduct and inappropriate behaviour,
- helping to verify incidents on college grounds to support an evidence-based response,
- reassuring students, staff and visitors that they are protected when on college grounds, and
- identifying breaches of the Catholic Education South Australian Policies - Behaviour Education and Personal Responsibility Policy and Respectful Relationships Policy.

DEFINITIONS

Closed Circuit Television (CCTV) - means Closed Circuit Television and in the context of this document includes all equipment used to record and store video and/or audio for the purposes of surveillance and protection of college property.

Vape Detection – means a system designed to detect atmospheric particles and loud noises that may indicate the use of e-cigarettes or inappropriate behaviour. No video is collected, and the system does not store audio data. The system only sends and records alerts.

SACCS – means the South Australian Commission for Catholic Schools

Staff - means any employee of CESA, including contractors, casual staff and outsource provided staff with contact with CESA provided ICT facilities.

Surveillance - means audio, optical and alert surveillance and includes the use of CCTV and Vape Detection.

SCOPE OF PROCEDURE

Ongoing Management Responsibility

The Principal is responsibility for the ongoing management of the Surveillance Devices within the College.

The Principal will be responsible for:

- controlling the operation of the Surveillance Devices is to ensure that it complies with the Australian Privacy Act (Cth) and in accordance with the Australian Privacy Principles (APPs); and within the Catholic Education South Australia (CESA) CCTV Video & Audio Surveillance Policy
- ensuring CCTV cameras are not installed in prohibited locations,
- ensuring that clearly identifiable warning signs with the message: 'Security Notice – electronic surveillance protects this property' are installed at appropriate entry points and throughout the College so that persons can be reasonably be expected to be aware that Surveillance is in operation, and
- supporting the maintenance and upgrade of Surveillance Devices when necessary.

Operating Requirements

The College will regulate access to Surveillance content in the following manner:

Requests to access Surveillance located at the College must be by written approved from the Principal.

All employees involved in the operation of the Surveillance Devices are expected to exercise care to ensure appropriate viewing and to prevent improper disclosure of the recorded material.

Surveillance content must only to be viewed by authorised personnel for Surveillance Device management and if there is a reasonable belief that an incident has occurred, and that the surveillance content may assist in identifying what had occurred and who may be involved.

The request for access to Surveillance content will be in writing.

If this access is for ongoing administration and maintenance of the Surveillance Devices the document will need to include the following information:

- date(s) access required,
- reason why access is required,
- name and position

If this access is in relation to an incident that has occurred, the document will need to include the following information:

- date access requested,
- name and position,

- date of the incident,
- time of the incident,
- location of the incident,
- reason why the content has been requested, and
- the names of those involved (if applicable).

All employees must be briefed on these requirements.

The Principal is required to maintain a register of who has accessed the College Surveillance and when. The register must be stored in a secure location.

Prohibited Use of Surveillance Devices

CCTV cameras must not be used in the following prohibited areas:

- toilets,
- change rooms,
- dressing rooms,
- bedrooms,
- first aid/sick bays, and
- showers.

Vape Detection systems do not record video or store audio and therefore can be installed in the above areas listed.

Hidden or covert Surveillance Devices are strictly prohibited.

Access to and Disclosure to Third Parties

All employees must be made aware of the restrictions set out in the CCTV and Vape Detection Policy and this procedure in relation to access and disclosure of recorded images.

Disclosure of Surveillance to third parties should be limited to the following classes of persons/agencies:

- disclosure to the police or officers of an investigating agency for the purposes of a relevant lawful investigation,
- disclosure authorised by a judge,
- disclosure to the person who was a party to the activity or their parent/guardian,
- disclosure with consent of each person involved in the recorded activity, and
- disclosure in relation to a situation in which a person is being subjected to violence or there is an imminent threat of violence to a person.

A register is to be kept of who has accessed the Surveillance and when.

The Principal should seek guidance from their School Performance Leader in relation to the release of footage to third parties.

Storage of Surveillance Content

Surveillance is to be kept for a maximum of 90 days.

When Surveillance is used to investigate and document specific or significant incidents, including an incident or alleged incident of child sexual abuse, the content must not be destroyed and must be stored in a secure location indefinitely.

If no request has been made to access content and no specific or significant incidents have taken place, the stored data can be overwritten after a minimum of 30 days.

CCTV content is to be stored on a designated secure server.

Access to content must be restricted to network administrators only who have written consent from the Principal.

Reporting Criminal Damage

Criminal activities and damage are to be reported without delay to the Principal who with the assistance of the School Principal Leader, will determine if Police involvement is required.

This information is used to implement security initiatives and other strategies to assist the College.

Managing Concerns and Complaints

Complaints about the College's Surveillance system should be managed in accordance with the processes outlined in the College Complaint Response and Resolution Procedure.

If a person is not satisfied that their complaint has been resolved by the College, or if their complaint is about the Principal, they may refer their complaint to the CESA office by following the CESA Complaint Response and Resolution Procedure.

Complaints about the College Surveillance system should be made in writing.

St Mark's College Revision Record

Document Title	CCTV and Vape Detection Policy
Document Date	November 2023
Review Date	November 2027