CLOSED CIRCUIT TELEVISION (CCTV) POLICY

Purpose & Scope:

(1) The Closed-Circuit Television (CCTV) Policy establishes the principles and operational procedures for the installation and use of CCTV by Trinity Catholic College Lismore.

(2) This Policy applies to all College staff and students. It also applies to contractors, service providers, clients, customers and visitors.

(3) This Policy does not apply to any recording or screening of liturgies or ceremonies conducted by the College.

Relevant to: All Members of Staff

Responsible Officer(s): Operations Manager

Date of Introduction: July 2024

Modification History:

Related Documents:

Related Forms:

POLICY STATEMENT

The College is committed to providing a safe and secure learning and working environment. Where necessary and appropriate the College will use CCTVs to protect people and assets in and around College property, while also respecting and protecting the individual's right to privacy. The use of CCTV is part of an integrated security approach that includes a number of strategies, including access controls, lighting, alarms and security staff.

DEFINITIONS:

(1) The following definitions apply to this Policy:

a. Closed Circuit Television (CCTV) means any combination of cameras, lenses, video/digital recorders and/or accessories installed for the purpose of monitoring and or recording visual activity.
b. Authorised User means a person authorised by the Operations Manager, or their nominee and the College's contracted security personnel.

Installation and Method of Operation

(2) Use of CCTVs is strictly restricted to activities which are:

a. reasonably necessary;
b. for lawful purposes; and
c. directly related to the College's functions or activities.

Responsibility

(3) The Operations Manager is responsible for the overall management of the College's CCTVs and has authority to amend or review the network from time to time.

Installation

(4) The following conditions apply to the installation of CCTVs:

a. The approval of the Operation's Manager must be obtained before the installation of a new camera;
b. CCTV cameras can only be installed by persons who are appropriately licensed under any relevant legislation,
c. CCTV cameras must not be hidden and must not be located.
    i. so as to capture images from private property adjacent to the College's; or
    ii. in any change room, toilet facility, shower or other bathing facility.
d. All CCTV controls, monitors and recorders must be located in a secure area.
e. Access to CCTV cameras will be limited only to Authorised Users.
f. All CCTV equipment will be integrated into the College's wider electronic security network to

enable effective monitoring by the College's security services.

Signage

(5) Signage indicating a CCTV system is in operation will be displayed at common entry points to each College Building and other high-volume traffic areas.

(6) The signage will:

a. be located within normal eye range, be clearly visible, distinctive, and located in a position that is well lit;
b. convey clearly that CCTV cameras are in place, preferably with the CCTV symbol; and
c. have been pre-approved by the Privacy Contact Officer as compliant with the requirements of the Privacy and Personal Information Protection Act 1998.

Monitoring

(7) The College CCTV footage is stored locally in a secure location within the SCU Data Centre, accessible only to Authorised Users. This area is monitored full time via security cameras as well as swipe card access recording.

(8) The ICT Manager, or their nominee, will ensure Authorised Users are aware of the College's policy and procedure before commencing work with the CCTV system.

(9) Access to the secure data storage location will be restricted to persons having a lawful and legitimate need of access. Prior approval of the Operation's Manager is required for individuals to gain access to the secure data storage location, with the exception of:

a. Authorised Users and;
b. law enforcement officers (refer clause (13)).

(10) Authorised Users must act with the utmost probity. The tracking or zooming in on any person must not be undertaken in a gratuitous or unreasonable manner. Camera operation is subject to audit and monitor operators may be called upon to explain their interest in a particular person.

(11) CCTV recorded information must be:

a. used only for the purpose for which it was approved to be collected (or as otherwise authorised or required by law);
b. stored securely in a secure location in the SCU Data Centre;
c. accessed only by Authorised Users;
d. restricted by user ID and password authentication (i.e. the use of generic user IDs, passwords or sharing of user IDs and passwords is not permitted);
e. clearly auditable and allow for the identification of individuals accessing the recorded information;
f. retained for a minimum of 14 days;
g. disposed of in a secure manner; and
h. protected from unauthorised access, use or disclosure.

(12) The ICT Manager will be responsible for monitoring compliance with the CCTV Policy and will report annually to the Operation's Manager regarding the use and management of the CCTV system.

Obtaining authorised access to data

(13) Images may be released to the Police Service or other law enforcement agencies in

compliance with relevant legislation. All requests made by the Police Service or other law enforcement agencies should be referred to the Operations Manager who will advise the College Privacy Officer of the request and its result using the Law Enforcement Information Access Form.

(14) The College may release images and/or recordings to third parties, other than law enforcement, but will only do so if authorized or required to by the Privacy and Personal Information Protection Act 1998. All other requests to view recorded information will be assessed in accordance with that Act and the Privacy Policy.

Complaints

(15) Privacy related CCTV complaints will be managed in accordance with the College's Privacy Policy.

(16) All other complaints will be managed in accordance with the College's Complaints Policy.

PROCEDURES

Monitoring (Operation)

(17) The CCTV system will generate a live feed which will be visible in the ICT Hub and then only by individuals who have authorisation to use the secure login. Access to the ICT Hub is via a personally coded swipe card and only authorized persons have access to ICT Hub and the secure feed..

Disposal

(18) Recordings and data produced by the CCTV system will be retained for a period of 14 days. The Operations Manager may determine to retain recordings, and data produced by the CCTV system for more than 30 days where it is allowable to do so under this Policy and the College Privacy Policy. Other than that, CCTV footage is automatically overwritten after 14 days.

Training

(19) Staff responsible for Security at the College will receive training with regards to the capabilities of the CCTV system installed. This training will include:

a. camera locations;
b. the responsibilities of Authorised Users when viewing recordings and making recommendations regarding further review;
c. this Policy;
d. the College Privacy Policy; and
e. all relevant legislation.

Authorised Users:

The following staff are deemed Authorised Users:

- Principal or their delegate;
- Members of the Leadership Team; and,
- ICT and Operations Managers.