Closed Circuit Television (CCTV) Procedure

Section 1 - Audience

(1) Staff, students, and visitors to the University of Newcastle (University) at all University premises.

Section 2 - Purpose

(2) This procedure outlines how the University manages and uses CCTV systems, footage and data, as defined by the CCTV Policy (Policy), and should be read in conjunction with the Policy.

(3) This procedure does not apply to streaming of live video or other installations which may occur during conferences, meetings, exhibitions or other University activities.

Section 3 - Definitions

(4) Definitions that are specifically related to this document and the CCTV Policy are outlined in the CCTV Policy.

Section 4 - Installation of CCTV

(5) The installation of CCTV systems or cameras must be:

a. undertaken by persons who are appropriately licensed under the Security Industry Act 1997 No 157(NSW);
b. in accordance with the requirements of the CCTV Policy; and
c. in accordance with Information Security Policy and its associated documents.

(6) The decision to install CCTV systems may be informed by community consultation.

(7) The installation of CCTV systems or cameras, or the relocation of CCTV cameras, must be authorised in writing by the Director, Infrastructure and Facilities Services.

(8) The Security Manager is responsible for ensuring that installation of CCTV systems and cameras meets the requirements of the Privacy and Personal Information Protect Act, the CCTV Policy, and this procedure.

Signage

(9) Signs indicating the operation of CCTV will be displayed near:

a. or below each CCTV camera and at entry points to the University campus; or
b. the entry point to University buildings that are off-campus.

(10) The signage must:

a. comply with the notification requirements of the Privacy and Personal Information Protection Act 1998;

b. be clearly visible;
c. be located in areas with good lighting;
d. be placed within normal eye range;
e. be large enough so the text can be read;
f. be easy to understand;
g. use worded text (such as CCTV 24 Hour Surveillance) and also symbols, such as an image of a camera; and
h. indicate when the area is being monitored, for example, 24 hours per day.

Notification Requirements

(11) Where CCTV is newly introduced to University premises, in addition to the implementation of signage, the University will give its affected employees at least 14 day's written notice of the operation of the CCTV system prior to its activation (unless a shorter period of notice is agreed to by the employees). This notice will indicate:

a. the kind of surveillance to be carried out;
b. how the surveillance will be carried out;
c. when the surveillance will commence;
d. whether the surveillance will be continuous or intermittent;
e. whether the surveillance will be for a specified limited period or ongoing; and
f. where the Closed Circuit Television (CCTV) Policy and Procedure can be found on the University's website.

(12) If use of the CCTV system has already commenced when an employee is first employed, the notice to that employee must be given before the employee commences work on University premises.

Section 5 - Access

Requests for Access to CCTV Footage

(13) Requests for access to CCTV footage will be considered by the Security Manager or their nominee for requests relating to the investigation of incidents or undesirable behaviour. Such requests must be made in writing to the Security Manager. The request will be considered in accordance with the Privacy and Personal Information Protect Act 1998, the CCTV Policy, and other relevant University policies.

(14) Subject to consultation with the Privacy and Right to Information Manager, and the approval of an authorised delegate, access may be granted by the Security Manager, or their nominee, where the use or disclosure of CCTV footage:

a. is for a legitimate business activity of function of the University, including those related to staff, students or visitors;
b. is for a purpose that is directly or indirectly related to civil or criminal proceedings;
c. is believed to be reasonably necessary to avert an imminent threat of serious violence to a person or persons, or substantial damage to property;
d. for the purposes of investigation of an incident or undesirable behaviour involving one or more staff or students; or
e. is to a law enforcement agency in connection with the detection, investigation, or prosecution of an offence.

(15) The Security Manager may place conditions on authorised access to CCTV footage.

(16) Requests for access to CCTV footage, other than those outlined in Clause 14, must be made in

accordance the Privacy and Personal Information Protection Act 1998 (PPIPA) or Government Information (Public Access) Act 2009 (GIPA). Instructions for how to make such requests can be found at GIPA Requests.

(17) A log of persons who have been given copies of CCTV footage, or have had access to CCTV footage will be maintained by the Security Manager.

Viewing Access

(18) Authorised access to view CCTV footage ("viewing access") must occur in:

a. the Security Control Room; or
b. a designated space with capabilities for footage review.

(19) Access to the Security Control Room or viewing access by law enforcement agencies will be in accordance with the principles of the University's Privacy Management Plan, and generally:

a. if it is reasonable to believe there is an imminent threat or risk of harm, access may be granted by the Control Room Operator with responsibility for monitoring the system at the time; or
b. if it is reasonable to believe there is a serious threat or risk of harm, access may be granted by the Security Manager.

(20) Initial requests made for access to footage by law enforcement officers under circumstances outlined in Clause 20 must be confirmed in writing to the law enforcement agency, nominating the applicable event reference number. See also "Access to the Security Control Room".

Shared Access

(21) Copies of CCTV footage may be shared ("shared access"), subject to authorisation under the applicable University procedure and/or delegated authority. Shared access must be made via a physical digital storage device which can only be released to:

a. law enforcement officers; or
b. other authorised persons where requested under a Government Information Public Access request or another legislative instrument.

Access to CCTV Data

(22) Requests for CCTV data should be sent via email to the Security Manager.

(23) Approved access to CCTV data must be in accordance with the provisions of the CCTV Policy.

Access to CCTV System

(24) Access to the CCTV system is granted by the Security Manager or their nominee.

(25) System access is controlled by the allocation of an individual user name and password.

(26) Access permissions may include rights to control, view, store, and dispose of recordings. The Security Manager is responsible for determining the access permissions for groups of users.

(27) The Security Manager is responsible for ensuring regular review of user access and permissions.

Access to the Security Control Room

(28) Access to the Security Control Room provides viewing access to live footage. Access to the Security Control Room must be authorised by the Security Manager, or their nominee, in accordance with this procedure. A register of persons authorised to access the Security Control Room will be maintained by the Security Manager and will include details of the:

a. person's name and their contact details;
b. date of authorisation;
c. authoriser's name and signature;
d. reason for access; and
e. date and time of access.

(29) Access to the Security Control Room must be subject to explanation of and agreement to the privacy and confidentiality requirements of the University.

Section 6 - CCTV Storage and Record Management

(30) CCTV footage, and all other records relating to access to CCTV footage, systems, and data must be stored and managed in accordance with the Policy, the Information Security Policy and the Records Governance Policy.

Destruction of CCTV Footage

(31) The CCTV system sanitises all un-bookmarked footage after 28 days by an automatic process of overwrite. The Security Manager is responsible for this process, including the monitoring and maintenance of the relevant system logs.

(32) The Security Manager is responsible for reviewing bookmarked footage and determining if it is required by the University or a law enforcement agency.

(33) Bookmarked CCTV footage and CCTV data logs must be retained for a minimum of 7 years after record completion and then destroyed in accordance with the Records Governance Policy and the University's delegations of authority (see Delegations Register).

(34) Where the bookmarked CCTV footage becomes part of legal proceedings the footage will only be destroyed when the related legal records are destroyed.

Disclosure of CCTV Footage

(35) Delegates who hold authority to release information, including but not limited to applications made under the GIPA or PPIPA Acts, which may include disclosure of CCTV footage, must do so in accordance with the relevant legislation and the University's Privacy Management Plan and Records Governance Policy.

Section 7 - Maintenance

(36) The Security Manager is responsible for ensuring that:

a. the CCTV system and cameras are subject to a regular and appropriate maintenance schedule and response, to ensure continuity of operation; and
b. that any person engaging in maintaining the CCTV system is appropriately licensed as required by the Security

Industry Act, 1997.

Section 8 - Monitoring Live Feed

(37) The CCTV system will generate live feed which is visible in the Security Control Room.

(38) The Security Control Room will be used for the purpose of monitoring the CCTV system.

(39) Where use of CCTV footage is authorised under the CCTV Policy, Control Room Operators will monitor the CCTV system to proactively identify and respond to emerging situations and to identify at any point where the live feed is compromised, or where the CCTV system is not operating at an optimal level.

(40) Control Room Operators are not permitted to zoom in on students or staff, except for the authorised purposes described in the CCTV Policy.

(41) The Security Manager is responsible for ensuring that Control Room Operators are appropriately licensed as required by the Security Industry Act, 1997.

Section 9 - Removal of CCTV Cameras

(42) A decision to remove a CCTV camera may occur when it is determined that the camera is no longer effective or required.

(43) The Director, Infrastructure and Facilities Services may authorise the removal of CCTV cameras.

Section 10 - Complaints

(44) Any person who believes a CCTV camera may be in use on University premises, other than in accordance with the CCTV Policy, or this procedure, should notify the Security Manager via email to Security-Services@newcastle.edu.au.

(45) All other complaints regarding CCTV should be made in accordance with the University Complaint Management Policy and associated procedure.

(46) Concerns and issues regarding the CCTV system can be made to the Associate Director, Campus Services.

Section 11 - Training

(47) The Security Manager will ensure that all Control Room Operators, members of the University Security Management team, and the contracted Security Supervisor receive training to ensure an appropriate level of understanding of:

a. the CCTV Policy and this procedure;
b. the capabilities and operation of the CCTV system. This training will include the location of the cameras and the responsibility of authorised officers when viewing recordings and making recommendations regarding further review;
c. obligations under PPIPA and GIPA; and
d. standard operating procedures.

Status and Details

Status	Current
Effective Date	3rd December 2024
Review Date	3rd December 2027
Approval Authority	Chief Operating Officer
Approval Date	25th November 2024
Expiry Date	Not Applicable
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Kevin McCarthy Director, Infrastructure and Facilities Services Infrastructure and Facilities Services

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"Delegate" - (noun) refers to a person occupying a position that has been granted or sub-delegated a delegation of authority, or a committee or body that has been granted or sub-delegated a delegation of authority.