Closed Circuit Television (CCTV) and Security Recordings Operational Procedure

Section 1 - Audience

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

Section 2 - Purpose

(2) This Procedure outlines how the University manages and uses Closed Circuit Television (CCTV) and security recording systems, footage and data, as defined by the Closed Circuit Television (CCTV) and Security Recordings Operational Policy (Policy), and should be read in conjunction with the Policy.

(3) This Procedure should be read in conjunction with the Closed Circuit Television (CCTV) and Security Recordings Operational Policy.

Section 3 - Definitions

(4) Definitions that are specifically related to this document and the Closed Circuit Television (CCTV) and Security Recordings Operational Policy are outlined in the Closed Circuit Television (CCTV) and Security Recordings Operational Policy.

Section 4 - Installation of CCTV and Security Recording Systems

(5) The installation of systems must be:

a. undertaken by persons who are appropriately licensed under the Security Industry Act 1997(NSW);
b. in accordance with the requirements of the Closed Circuit Television (CCTV) and Security Recordings Operational Policy; and
c. in accordance with Digital Security Policy and its associated documents.

(6) The decision to install CCTV systems may be in response to community feedback.

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

(8) The Senior Manager Security is responsible for ensuring that installation of CCTV and security recording systems meets the requirements of the Privacy and Personal Information Protect Act, the Closed Circuit Television (CCTV) and Security Recordings Operational Policy, the Privacy Management Plan and this procedure.

Signage

(9) Signs indicating the operation of CCTV or security recordings will be displayed:

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

(10) The signage should, where practicable:

a. comply with the notification requirements of the Workplace Surveillances Act;
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 new cameras or security recording methods are 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 prior to activation (unless a shorter period of notice is agreed to by the employees). This notice will indicate:

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

(12) If use of the security recording 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 Footage

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

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

a. is for a purpose that is directly or indirectly related to civil or criminal proceedings;
b. is believed to be reasonably necessary to avert an imminent threat of serious violence to a person or persons, or substantial damage to property;
c. for the purposes of investigation of an incident or undesirable behaviour; or
d. is to a law enforcement agency in connection with the detection, investigation, or prosecution of an offence.

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

(16) Requests for access to 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 footage, or have had access to footage will be maintained by the Senior Manager Security.

Viewing Access

(18) Authorised access to view 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 Senior Manager Security.

(20) Requests made for access to footage by law enforcement officers 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 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 Data

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

(23) Approved access to data must be in accordance with the provisions of the Closed Circuit Television (CCTV) and Security Recordings Operational Policy.

Access to CCTV System

(24) Access to the CCTV system is granted by the Senior Manager Security 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 Senior Manager Security is responsible for determining the access permissions for groups of users.

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

Access to Body Worn Cameras (BWC's)

(28) BWC's must be maintained in a secure controlled environment. Access to BWC's is the responsibility of the Senior Manager Security.

(29) Allocation of individual BWC's to Authorised Security Officers must generate a formal record that provides the following information:

a. the asset or serial number of the BWC provided to the Authorised Security Officer;
b. the date the BWC was allocated;
c. the Authorised Security Officer the BWC was allocated to;
d. the purpose for allocating the BWC;
e. the date the BWC was returned.

Access to the Security Control Room

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

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

Section 6 - Record Management

(32) Footage, and all other records relating to access to systems, footage and data must be stored and managed in accordance with the Closed Circuit Television (CCTV) and Security Recordings Operational Policy, the Digital Security Policy and the Records Governance Policy.

BWC Operation Records

(33) The Senior Manager Security is responsible for ensuring adequate records of BWC activation are created, and retained in accordance with the requirements of this Procedure.

BWC Footage

(34) BWC footage must be downloaded as soon as practicable after recording an event or incident. Authorised Security Officers are responsible for returning the BWC to a secure location as soon as practicable after the event or incident for which its use was authorised.

Destruction of Footage

(35) All un-bookmarked footage will be sanitised after 28 days by an automatic process of overwrite. The Senior Manager Security is responsible for this process, including the monitoring and maintenance of the relevant system logs.

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

(37) The Senior Manager Security is responsible for reviewing BWC footage as soon as possible after an event is recorded, and determining if it is required by the University in accordance with the Closed Circuit Television (CCTV) and Security Recordings Operational Policy. In the event the footage is determined as not being required by the University or a law enforcement agency, the BWC footage must be deleted, subject to approval by an authorised delegate. An appropriate record of all deleted BWC footage must be kept by the Senior Manager Security.

Footage Retention

(38) Bookmarked footage and 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).

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

Disclosure of Footage

(40) Delegates who hold authority to release information, including but not limited to applications made under the Government Information (Public Access) Act 2009 or Privacy and Personal Information Protection Act 1998 Acts, which may include disclosure of footage, must do so in accordance with the relevant legislation and the University's Privacy Management Plan and Records Governance Policy.

Section 7 - Maintenance

(41) The Senior Manager Security is responsible for ensuring that:

a. the CCTV and security recording systems and cameras are subject to a regular and appropriate maintenance schedule to ensure continuity of operation; and
b. that any person engaging in maintaining the CCTV and security recording system is appropriately licensed as required by the Security Industry Act, 1997.

Section 8 - Monitoring Live Feed

(42) The CCTV system will generate live feed which is visible in the Security Control Room. BWC’s may generate live feed visible in the Security Control room.

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

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

(45) Control Room Operators are not permitted to zoom in on students or staff, except for the authorised purposes described in the Closed Circuit Television (CCTV) and Security Recordings Operational Policy.

(46) The Senior Manager Security 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

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

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

Section 10 - Body Worn Camera Standard Operating Procedure

(49) The Senior Manager Security is responsible for ensuring that a Standard Operating Procedure for use of BWC's is developed, operationalised, reviewed on a regular basis, and effective.

(50) The Standard Operating Procedure must be informed by a privacy impact assessment.

(51) The Standard Operating Procedure for use of BWC's must be accessible to Authorised Security Officers.

Section 11 - Complaints

(52) Any person who believes CCTV or security recording may be in use on University premises, other than in accordance with the Closed Circuit Television (CCTV) and Security Recordings Operational Policy, or this procedure, should notify the Senior Manager Security via email to Security-Services@newcastle.edu.au.

(53) All other complaints regarding CCTV or security recordings within the scope of the Closed Circuit Television (CCTV) and Security Recordings Operational Policy and this Procedure should be made in accordance with the University Complaint Management Policy and associated procedure.

(54) Concerns and issues regarding the CCTV system can be made to the Associate Director, Campus Services via security-services@newcastle.edu.au.

Section 12 - Training

(55) The Senior Manager Security is responsible for:

a. identifying and nominating suitable persons for BWC device training, and maintaining a register of those persons who have completed the training;

b. ensuring a sufficient number of Security Officers have completed BWC device training at any given time;
c. ensuring that trained Authorised Security Officers undergo regular refresher BWC device training on an annual basis.

(56) Body Worn Camera device training will include:

a. all technical aspects of the equipment being used;
b. ethical and appropriate use;
c. authorised uses of BWC's;
d. privacy and other legislative requirements of using BWC's; and
e. standard operating procedures for use of BWC's.

(57) Only trained persons, in accordance with Clause 58, are authorised to use a BWC for the purposes of security recording.

(58) The Senior Manager Security 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 Closed Circuit Television (CCTV) and Security Recordings Operational 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 Privacy and Personal Information Protection Act 1998 and Government Information (Public Access) Act 2009; and
d. standard operating procedures.

Status and Details

Status	Current
Effective Date	28th October 2026
Review Date	25th March 2029
Approval Authority	Chief Operating Officer
Approval Date	27th October 2026
Expiry Date	Not Applicable
Responsible Executive	Morven Cameron 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.

"Campus" - means any place or premises owned or controlled by the University, but may also specifically refer to a designated operating location such as the Callaghan Campus.

"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.

"Delegated authority" - refers to the specific description of the authority that is delegated or sub-delegated to a holder.