Closed Circuit Television (CCTV) and Security Recordings Operational Policy

Section 1 - Audience

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

Section 2 - Purpose

(2) This Policy:

a. outlines how the University operates and manages Closed Circuit Television (CCTV) and security recordings;
b. in addition to other mechanisms, provides notice to employees under the Workplace Surveillance Act 2005 (NSW).

(3) This Policy should be read in conjunction with:

a. Closed Circuit Television (CCTV) and Security Recordings Operational Procedure;
b. Campus Access Policy;
c. Privacy Management Plan; and
d. Privacy Policy.

Section 3 - Scope

(4) This Policy applies to:

a. all users of the University premises;
b. CCTV and security recording systems installed on University premises;
c. CCTV and security recording footage; and
d. CCTV and security recording data collected.

(5) The Policy does not apply to streaming of live video or other video or audio installations which may occur during ceremonies, conferences, meetings, exhibitions, or other University activities.

(6) This Policy does not apply to monitoring of digital assets – please see Digital Technology Conditions of Use Policy.

Section 4 - Definitions

(7) In the context of this document and the Closed Circuit Television (CCTV) and Security Recordings Operational Procedure:

a. “Authorised Security Officer” is a Security Officer who has received appropriate training to use a Body Worn

Camera (BWC) and has been nominated to use the BWC by the Senior Manager Security or Team Leader Security Operations;

b. “BWC activation” refers to the decision to commence recording via a BWC. Recording may be audio and/or visual;
c. “cctv or security recording data” or “data” refers to facts and statistics collected from the CCTV or security recording system, and/or through image processing, that does not contain personal information or images;
d. “employee” is as defined by the Workplace Surveillance Act, as amended from time to time, or as per any replacing legislation;
e. “incident” refers to any activity that may impact on the health, safety, security or welfare of persons on University premises;
f. “CCTV and security recording footage” or “footage” refers to the images, audio and/or audiovisual data captured by a CCTV or security recording system and the metadata that is integral to establishing the context, validity and authenticity of the footage. Footage is considered a record under the State Records Act (NSW) and is subject to the Records Governance Policy;
g. “CCTV and security recording system” or “system” means a device or group of devices and applications used for live security recording including fixed cameras; pan, tilt and zoom closed circuit television (CCTV) cameras; and body worn cameras (BWC);
h. “University premises” includes all land, buildings, facilities, and other property in the possession of or owned, used, or controlled by the University, including without limitation the residential colleges; and
i. “visitors” means all persons who are not staff or students of the University but who are attending a University campus or premises.

Section 5 - Policy Principles

(8) CCTV and security recording forms part of the University's integrated approach to ensuring safety and security.

(9) The University will comply with all relevant laws in relation to CCTV and security recording.

(10) CCTV and security recording systems may be operated on University premises.

(11) CCTV and security recording systems may be operated by the University or by the University's third party security providers.

(12) CCTV may or may not be continually monitored.

Authorised Purposes

(13) The University operates CCTV and security recording systems and may use their footage to help enhance the health, safety, security, and welfare of persons who enter University premises.

(14) Body worn cameras may be used to capture accurate versions of an emergency, incident or planned event or as authorised by the Senior Manager Security, or their nominee.

(15) Footage may also be used for related purposes, including:

a. the investigation of incidents, including suspected illegal activity that may compromise the health, safety, security and welfare of persons who enter University premises; and
b. identification of persons involved in any breach(es) of University policy including for the purpose of disciplinary action in relation to incidents involving staff or students.

(16) Data may be used for the purposes of campus planning and management.

CCTV Camera Locations

(17) The location of CCTV cameras will be determined by a risk based approach taking into consideration areas:

a. with high incident rates; and
b. where there is a risk of incidents.

(18) The Director, Infrastructure and Facilities Services may approve the installation, relocation, or removal of CCTV cameras if it is considered reasonably necessary for one or more of the purposes set out in this policy.

(19) In complying with the Workplace Surveillance Act 2005, the University strictly prohibits CCTV or security recording of an employee in a change room, toilet facility or shower, or other bathing facility. In relation to any individual, staff, student or the general public, the CCTV or security recording of a person in a change room, toilet facility, shower or other bathing facility would be considered a serious invasion of privacy.

Signage

(20) The University will install and maintain appropriate signage to indicate that CCTV or security recording may be in operation, in accordance with the Closed Circuit Television (CCTV) and Security Recordings Operational Procedure.

Body Worn Cameras (BWC's)

(21) BWC's may be worn by authorised Security Officer's for authorised purpose, as outlined in clauses 13 to 16.

(22) BWC's must be highly visible and must not be operated covertly.

(23) Authorised Security Officers must communicate the commencement of recording of a BWC prior to commencing recording, as far as reasonably possible.

(24) Where an incident requires it, BWC's may be used with or without consent of any person(s) who may be captured in the footage.

Collection of Footage

(25) The collection of footage, and its management, will be in accordance with relevant privacy laws and the Privacy Management Plan.

Access to Footage

(26) The business unit responsible for retrieval of footage is Safety and Security Services at the Callaghan Campus.

(27) Access to footage will be in accordance with the Privacy and Personal Information Protection Act, the Privacy Management Plan and the Closed Circuit Television (CCTV) and Security Recordings Operational Procedure.

(28) The Senior Manager Security, or their nominee, will ensure only persons who are authorised by an appropriate delegate are provided access to footage.

Use of Footage

(29) Footage must only be used or disclosed for the purpose for which it was collected, or as otherwise permitted under this Policy.

Access to Data

(30) The Senior Manager Security is responsible for authorising access to data.

Retention of Footage and Data

Footage

(31) Footage will be maintained for no more than 28 calendar days. The Senior Manager Security may determine to bookmark and retain footage for more than 28 calendar days where:

a. the footage may be of evidentiary value in relation to a reported or detected incident;
b. the University has been asked by a law enforcement agency to retain or produce the footage;
c. the footage has been copied by a Control Room Operator for further review and the review is not complete; or
d. the University's Legal and Governance Services unit advises that the footage should be retained.

(32) Footage retained under clause 31 will only be retained for as long as is reasonably necessary.

(33) For any footage retained, an appropriate duration of the footage must be retained to show the context of any individuals' actions.

Data

(34) Data may be copied and stored for later use in relation to analysis and planning. Data will be stored for a duration that is commensurate with the purpose for which it is to be used. Once the data has been used it will be deleted.

Destruction of Footage and Data

(35) Destruction of footage and data must be in accordance with the Closed Circuit Television (CCTV) and Security Recordings Operational Procedure where relevant, and comply with all relevant policies including the Records Governance Policy.

Public Display of Images

(36) The Director, Infrastructure and Facilities Services may authorise the public display of an image or footage from CCTV or security recording to:

a. seek assistance from members of the University community to identify a person reasonably suspected or known to have committed an offence; or
b. warn people of a danger to personal safety associated with such a person.

CCTV and Security Recording Register

(37) The University will maintain a register of all CCTV and security recording systems in operation.

Compliance

(38) Staff or students who fail to comply with the requirements of this policy, or who are found to tamper or interfere with CCTV or security recording systems, may be found to be in breach of the Student Code of Conduct or Staff Code of Conduct and may be subject to disciplinary action.

(39) Contractors found to be in breach of this policy or its associated documents may be subject to remedial action under the provisions of any associated contract or agreement.

Complaints Resolution

(40) Complaints in relation to matters that are subject to this policy must be made in accordance with the Closed Circuit Television (CCTV) and Security Recordings Operational Procedure.

Roles and Responsibilities

(41) The Director, Infrastructure and Facilities Services is responsible for the University CCTV and security recording systems and the implementation of relevant standard operating procedures.

(42) The Senior Manager Security is responsible for managing the systems in accordance with this policy, including the review of the systems at least every two years that entails reviewing:

a. the effectiveness and location of each CCTV camera on University premises and the need to locate a camera at that point; and
b. relevant policies and procedures; and
c. relevant standard operating procedures.

(43) Security personnel are responsible for the operation of the systems in accordance with the relevant legislation, this policy and its associated procedure.

Status and Details

Status	Current
Effective Date	25th March 2026
Review Date	25th March 2029
Approval Authority	Chief Operating Officer
Approval Date	23rd March 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.

"Calendar days" - All days in a month including weekends and public holidays.

"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.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

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

"Disciplinary action" - When used in relation to staff of the University, this is as defined in the applicable and current Enterprise Bargaining Agreement, or the staff member's employment contract. When used in relation to students of the University, this refers to the range of penalties that may be applied under the Student Conduct Rule.

"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.

"Digital asset" - Means all or any information technology solution(s) (regardless of whether they are physical or software-based), and the facility(ies) that house them.