

Closed Circuit Television (CCTV) Procedure

Section 1 - Introduction

(1) The University installs and maintains a CCTV system in and around University grounds and buildings. Cameras are installed primarily to assist in ensuring the security of University campuses, persons and property.

(2) The use of the CCTV system and any recordings are subject to a number of legal obligations, including NSW workplace surveillance and privacy laws.

Section 2 - Audience

(3) Staff, students and visitors to the University of Newcastle.

Section 3 - Management of the System

Responsibility

(4) The Security Manager is responsible for the installation, operation, monitoring and maintenance of the CCTV system on University premises.

(5) Any member of staff who believes a surveillance camera may be in use on University premises other than in accordance with this procedure should notify the Security Manager.

Section 4 - Installation

(6) The installation of the CCTV system will be undertaken by persons who are appropriately licensed under the [Security Industry Act 1997 No 157](#) (NSW).

(7) No CCTV camera may be installed or its location varied unless the Director, Infrastructure and Facilities Services considers it is reasonably necessary for one or more of the purposes set out in the Policy.

Section 5 - Signage

(8) Signs indicating the operation of CCTV will be displayed near or below each CCTV camera and at entry points to the University campus.

(9) The signage must:

- a. comply with the notification requirements in section 10 of the [Privacy and Personal Information Protection Act 1998 No 133](#);
- b. be clearly visible (located near or below each CCTV camera and at entry points to the University);
- 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 whether the area is being monitored 24 hours per day.

Section 6 - Workplace Surveillance Act

(10) In addition to the implementation of signage, the University must give its 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 must 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.
- g. 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 on University premises.

Section 7 - Live Feed

(11) The CCTV system will generate a live feed which will be visible in a monitoring room.

(12) The monitoring room will be used only for the purpose of monitoring the CCTV system and access will only be available for authorised persons accessing the room with a personally coded swipe card.

(13) If the monitoring room is accessed by an authorised person who does not hold a swipe card they must sign in and sign out using a log book located in the room.

Section 8 - Recordings

Storage

(14) Recordings and data produced by the CCTV system will unless authorised by the Security Manager, be retained for a period of no more than 28 days.

(15) The Security Manager may determine to retain recordings, and data produced by the CCTV system for more than 28 days where:

- a. A incident has been reported or detected; or
- b. the University has been asked by a law enforcement agency to retain or produce the recordings or data; or
- c. the recording has been flagged by a Security Officer for further review and the review is not complete; or
- d. the University's Legal Office advises that the recording or data should be retained; or
- e. in such circumstances the recordings and data will only be retained for as long as is reasonably necessary.

(16) For any recordings or data being retained the appropriate length of footage should be preserved to show the context of an individual's actions.

Access

(17) The primary area for data retrieval and review will be in the University Security Office, Callaghan Campus.

(18) Only authorised persons will have access, and access will be on conditions set by the Security Manager.

(19) A log of persons who have or have had access to the CCTV recordings will be maintained by the Security Manager.

(20) Access to the CCTV system for control, view, storage and disposal of recordings is by individual user name and password.

Use or Disclosure relating to employees

(21) Use or disclosure of surveillance footage in relation to employees is permitted in the following circumstances:

- a. use or disclosure for a legitimate purpose related to the employment of employees by the University or the legitimate business activities or functions of the University;
- b. disclosure to a law enforcement agency in connection with the detection, investigation or prosecution of an offence;
- c. use or disclosure for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings; and
- d. use or disclosure reasonably believed to be necessary to avert an imminent threat of serious violence to persons or substantial damage to property.

Law Enforcement

(22) Access to the monitoring room for the CCTV system, or to recordings from the CCTV system to 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 Security Officer with responsibility for monitoring the system at the time;
- b. If it is reasonable to believe there is a serious threat or risk of harm, access may be granted by the Security Manager.

(23) Individuals may request access to footage from Surveillance Cameras under PPIPA or GIPA.

Public Display

(24) The Director, Infrastructure and Facilities Services, may authorise the public display of an image or recording from the CCTV system for the purpose of:

- a. seeking assistance from members of the University community in identifying a person reasonably suspected or known to have committed a serious offence; and
- b. warning people of a danger to personal safety associated with such a person.

Section 9 - Training

(25) All Security Officers at the University will receive training with regards to:

- a. the capabilities of the CCTV system installed on all University premises. This training will include the location of the cameras and the responsibility of authorised officers when viewing recordings and making recommendations regarding further review; and
- b. obligations under PPIPA and GIPA.

(26) Camera operators must not zoom in on students and staff, except for the authorised purposes described in the Policy and Procedure

Section 10 - Register

(27) The University will maintain a register of all CCTV cameras in operation.

Section 11 - Review

(28) A review of the CCTV system will be undertaken by the Security Manager every two years and will include:

- a. A review of each location of CCTV cameras on University premises and whether the need to locate a camera at that point is still required;
- b. A review of the Policy; and
- c. A review of this Procedure.

Section 12 - Roles and Responsibilities

(29) The Director, Infrastructure and Facilities Services is responsible for approving new CCTV Cameras or locations and the public display of CCTV recordings, in accordance with this Procedure.

(30) The Security Manager is responsible for the management of the CCTV System and authorised Security Officer, in accordance with this Procedure.

(31) Authorised Security Officer are responsible for the operation of the CCTV system in accordance with this Procedure.

Status and Details

Status	Historic
Effective Date	11th November 2014
Review Date	31st December 2019
Approval Authority	Vice-Chancellor
Approval Date	11th November 2014
Expiry Date	11th May 2021
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	David Toll Chief Operating Officer <hr/> 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.

"Law" - All applicable statutes, regulations, by-laws, ordinances or subordinate legislation in force from time to time anywhere in Australia, whether made by the Commonwealth, a State, a Territory or a local government and, where the context permits, includes the common law and equity.

"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.