CCTV PROCEDURES 2019

Issued by:	Director, Campus Infrastructure and Services
Dated:	8 August 2019
Signature:	
Name:	Greg Robinson

---

1 Purpose and application

(1) These procedures are to give effect to the *Privacy Policy 2017*.

(2) These procedures apply to:

(a) the University, staff and affiliates;

(b) all CCTV cameras operated by or on behalf of the University.

(3) These procedures do not apply to recording lectures or public events at the University.

2 Commencement

These procedures commence on 9 August 2019.

3 Interpretation

(1) Words and phrases used in these procedures and not otherwise defined in this document have the meanings they have in the policy.

authorised users	means users authorised by the Director, Campus Infrastructure and Services to configure, monitor, access and retain CCTV vision.
approved security contractors	means authorised installers or accredited security companies provided in the *CIS Security Services Standard.*
CSU	means Campus Security Unit.
CCTV	means closed circuit television, and refers to a network of video cameras that record images of individuals, with no sound.
control room	means the secure central location where CCTV monitors are viewed.
crisis	has the meaning provided in the *Serious Incident and Business Continuity Policy 2013*, which at the date of these procedures is:

	an incident of a severe nature that has the potential to seriously disrupt University business. It involves real or potential threat to life, or fatalities, and is likely to involve matters with the potential for substantial and ongoing impact on the reputation of the University and have serious implications for key University operations.
DCIS	means the Director, Campus Infrastructure and Services
law enforcement agency	means any of: • the NSW Police Force; • the police force of another Australian state or territory; • the NSW Crime Commission; • the Australian Federal Police; • the National Crime Authority; • the Director of Public Prosecutions of any state or territory or of the Commonwealth; • the NSW Department of Corrective Services; • the Police Integrity Commission; • the Independent Commission Against Corruption; or • the NSW Department of Juvenile Justice
privacy mask	means a configuration applied to a camera to restrict the detail or movement of CCTV vision through blurring or pixilation.
Proper Officer	means the person appointed to receive subpoenas on behalf of the University. At the date of these procedures, it is the University's Records Manager.
public spaces	means any of: • pedestrian corridors; • gathering areas; • emergency evacuation areas. • building foyers; • carparks; • public seating areas; • lifts; • stairwells; or • corridors.
restricted CCTV vision	means vision taken by a camera that is configured with a privacy mask.

serious incident has the meaning provided in the *Serious Incident and Business Continuity Policy 2013*, which at the date of these procedures is:

> a significant adverse event which affects the University, its staff, students, affiliates or visitors and which requires a University response. It involves significant disruption to University business or includes serious injury or threat to life. Any incident which involves one or more emergency service (for example, the police, ambulance, fire brigade) is a serious incident. This term is interchangeable with the terms critical incident or emergency.

staff recreation areas means:

- kitchens; or
- staff rooms.

staff work areas means, but is not limited to:

- staff workstations;
- laboratories;
- meeting rooms;
- photocopy rooms; and
- shared workspaces.

third parties includes:

- external solicitors;
- insurance companies; and
- law enforcement agencies.

University lands has the meaning given in the *University of Sydney (Campus Access) Rule 2009* which at the date of these procedures is:

> University lands includes any land or roads occupied or used in connection with the University, including the whole or part of any building or structure and any land or roads occupied or used in connection with the whole or part of any building or structure.

5 Purposes for which CCTV is employed

(1) CCTV recording on University lands must be:

(a) reasonably necessary; and

(b) lawful.

(2) CCTV may be installed and operated:

(a) to facilitate the safety and security of the University and the people accessing its lands and facilities;

(b) to minimise risk of access by unauthorised persons;

(c) for analytical purposes, to:

(i) map and record trends that occur; and

(ii) plan and distribute resources;

(d) for recording details of access to premises, including:

(i) the identity of individuals; and

(ii) time of access;

(e) for investigative or legal purposes, including for investigations in accordance with the *Resolution of Complaints Policy 2015*; and

(f) for planning, prevention, response or recovery from a serious incident or crisis.

6 CCTV operation

(1) All CCTV cameras on University lands must be operated in accordance with:

(a) the *Privacy Policy 2017;*

(b) the *Privacy Procedures 2018;*

(c) these procedures; and

(d) the *CIS Security Services Standard*.

(2) CCTV cameras may be installed at multiple points on University lands excluding:

(a) change rooms;

(b) toilet facilities;

(c) shower and bathing facilities; and

(d) as otherwise directed by legislation.

(3) CCTV cameras must not record staff work areas or staff recreation areas.

(a) CCTV cameras with fields of vision which would otherwise include such areas must be masked to exclude them.

7 Signage

(1) Signs notifying individuals that a CCTV camera is operating must be located at:

(a) all major entrances to the University;

(b) building entrances, including:

(i) carparks;

(ii) side entrances;

(iii) event spaces; and

(iv) cafes.

(2) Signs must:

(a) be clearly visible;

(b) appropriately lit, if necessary;

(c) be placed within normal eye range;

(d) identify the University as the operator of the CCTV;

(e) state when the CCTV is in operation;

(f) state whether CCTV is operated continuously;

(g) details of the purposes for which CCTV is employed;

(h) a statement that individuals are entitled to:

(i) access their own personal information recorded by the CCTV; and

(ii) how such access may be obtained;

(i) provide a website address where further information may be obtained;

(3) Information on the sign referred to in subclause (2)(g) must include:

(a) details of where copies of the *Privacy Policy 2017*, *Privacy Procedures 2018,* these procedures and the *CIS Security Services Standard* may be obtained; and

(b) details of how complaints or concerns may be raised.

8 Installing CCTV cameras

(1) The Vice-Principal (Operations) must approve the installation of new CCTV cameras in accordance with clause 5 of these procedures.

(2) CCTV cameras can only be installed by approved security contractors.

Note: see the *CIS Security Services Standard.*

(3) Prior to installation of a new CCTV camera, at least 14 days written notice must be given to students, staff and affiliates, stating:

(a) the kind of surveillance to be carried out;

(b) where the surveillance will be carried out;

(c) how the surveillance will be carried out;

(d) when the surveillance will start;

(e) whether the surveillance will be continuous or intermittent;

(f) whether the surveillance will be for a specified limited period or ongoing; and

(g) whether the surveillance is configured with a privacy mask to restrict CCTV vision.

(4) Only authorised users may configure or reconfigure a camera with a privacy mask.

9 Monitoring CCTV vision

(1) CCTV vision must only be monitored by authorised users:

(a) from the control rooms or, in exceptional cases, from dedicated security monitors in particular buildings; and

(b) only for purposes consistent with the *Privacy Policy 2017*, the *Privacy Procedures 2018* and these procedures.

(2) Where CCTV vision is monitored outside the control room:

(a) the monitors must be positioned as far as practicable to exclude viewing by the general public; and

(b) when operational, the monitors must be under the control of an authorised user.

10 Access to CCTV vision

(1) CCTV vision will not be used or disclosed, except:

(a) as required by law; and

(b) in accordance with the *Privacy Policy 2017* and the *Privacy Procedures 2018*.

(2) Authorised users may access CCTV vision only for purposes consistent with the *Privacy Policy 2017*, the *Privacy Procedures 2018* and these procedures.

(3) Individuals, other than authorised users, may apply for information about, or access to, CCTV vision under:

(a) the *Privacy and Personal Information Protection Act 1998* (NSW); or

Note: Contact: privacy.enquiries@sydney.edu.au

(b) *Government Information (Public Access) Act 2009* (NSW).

Note: Contact: gipa.enquiries@sydney.edu.au

(4) Third parties that require access to CCTV vision under subpoena, warrant or other court order should contact the Proper Officer.

Note: See: https://sydney.edu.au/legal/regulations/subpoenas.shtml

(5) Law enforcement agencies may be provided access to:

(a) the control rooms,

(b) dedicated security monitors located outside the control room;

(c) live CCTV vision;

(d) restricted CCTV vision; and

(e) retained CCTV vision

in accordance with the *Privacy Policy 2017*, the *Privacy Procedures 2018* and these procedures.

(6) The DCIS must approve all requests for access to restricted CCTV vision.

11 Retaining CCTV vision

(1) The CSU will retain copies of, and appropriately store, all requests for access to CCTV vision.

Note: See *Recordkeeping Policy 2017*

(2) Images will generally not be retained for more than 30 days, unless a valid request is received within 30 days from:

(a) a law enforcement agency; or

(b) for the purpose of conducting a preliminary assessment or investigation;

(3) Retained images must be:

(a) securely stored in the University's official records management system; and

(b) accessible only by authorised users in accordance with these procedures.

(4) When no longer required to be retained, images must be deleted securely and permanently in accordance with the *State Records Act 1998*

12 Recordkeeping and reporting

(1) **Authorised users.** The Manager, CSU, must establish and maintain a register to record:

(a) the names of authorised users;

(b) the date of authorisation;

(c) other relevant information, e.g. security number, and

(d) date of cessation of authorisation.

(2) **Access to the control room**. The Manager, CSU, must establish and maintain a register to record:

(a) authorised users who access the control room and the dates and times on which they do so; and

(b) all visitors who enter the control room, including:

(i) the visitor's organisation;

(ii) the reason for entry;

(iii) the date and time of entry and exit from the control room; and

(iv) the name of the authorised user who provides access.

(3) The register must be retained in the University's official records management system for a minimum of two years.

(4) **Access to dedicated security monitors located outside control room.** The Manager, CSU, must establish and maintain a register to record:

(a) authorised users who operate each security monitor, or group of monitors outside the control room and the dates and times on which they do so;

(b) all visitors who view the monitors, including;

(i) the visitor's organisation;

(ii) the reason for the viewing;

(iii) the date and time of viewing, including start and finish times; and

(iv) the name of the authorised user who permits the viewing.

(5) The register must be retained for a minimum of two years.

(6) **The configuration of CCTV cameras.** The Manager, CSU must maintain a record of:

(a) the configuration of each camera;

(b) whether the camera has a privacy mask;

(c) the date the privacy mask was configured;

(d) the authorised user who added, changed or removed the privacy mask;

(e) the reason for changing the camera configuration;

(f) requests for access to restricted CCTV vision;

(g) the release of restricted CCTV vision; and

(h) the purpose for extracting restricted CCTV vision.

(7) **Training.** The Manager, CSU must establish and maintain a register to record training undertaken by authorised users as required by clause 12 of these procedures, including:

(a) the name of authorised users who attended;

(b) the date of the training, including start and finish times; and

(c) the content of the training.

(8) Any authorised user who:

(a) provides access to the control room or to dedicated security monitors located outside control room to a visitor; or

(b) who changes the configuration of a CCTV camera;

is responsible for completing the register to record their activities prescribed by this clause.

(9) **Reporting.** The Manager, CSU must provide a report to the Director, Campus Infrastructure and Services at least every six months, which summarises the information recorded in the registers.

13 Training

(1) The Manager, CSU must require all authorised users to attend training at least annually on:

(a) the policy;

(b) the University's privacy and recordkeeping requirements; and

(c) these procedures.

14 Removing CCTV cameras

(1) The DCIS must approve the temporary or permanent cessation of use of any CCTV camera.

(2) CCTV cameras can only be removed by approved security contractors.

Note: See the CIS Security Services Standard.

(3) Subclauses (1) and (2) do not apply to the temporary removal of CCTV cameras for maintenance.

15 Inquiries and complaints

(1) Inquiries or complaints about privacy related matters should be directed to the University's Privacy Officer.

(2) All other inquiries or complaints should be directed to one of the following:

(a) DCIS;

(b) Manager, CSU.

Note: See the *Privacy Policy 2017* and *Privacy Procedures 2018*

NOTES

CCTV Procedures 2019

Date adopted:	8 August 2019
Date commenced:	9 August 2019
Administrator:	Simon Hardman, Head of Campus Security and Emergency Management
Review date:	8 August 2024
Rescinded documents:	
Related documents:	*Privacy Act 1988 (Commonwealth)* *Government Information (Public Access) Act 2009* *Privacy and Personal Information Protection Act 1998 (NSW)* *State Records Act 1988* *Workplace Surveillance Act 2005 (NSW)* *University of Sydney (Campus Access) Rule 2009* *Privacy Policy 2017* *Recordkeeping Policy 2017* *Resolution of Complaints Policy 2015* *Serious Incident and Business Continuity Policy 2013* *Privacy Procedures 2018* CIS Security Services Standard

AMENDMENT HISTORY

Provision	Amendment	Commencing