

Security and Access to University Premises Policy

Section 1 - Purpose

(1) This policy outlines security and access measures for Charles Sturt University's controlled areas and provides guidance to staff with administration responsibilities regarding security and access to Charles Sturt University (the University) premises. To ensure the security and safety of all staff, students and visitors and protection of University property; the University has the right to regulate and control access to and use of University premises, such regulation and control to include any person and vehicle(s) which may be within a person's control.

(2) The objectives of this policy are to:

- a. provide a safe and secure physical environment for staff, students, and visitors (including contractors and suppliers),
- b. protect University assets and property,
- c. ensure students, staff and visitors enjoy the social and academic benefits of the University,
- d. uphold the University's commitment to the freedom of speech and academic expression,
- e. prevent the University from being used as a forum to advocate any issue which may breach:
 - i. any University policy, or
 - ii. any Commonwealth, State or Territory law
- f. minimise the number, range and impact of incidents on teaching and research activities, infrastructure and people, and
- g. empower staff to appropriately respond to incidents and emergencies in accordance with documented operating procedures and manuals which are informed by this policy.

Scope

(3) This policy applies to all staff, students of the University and also to visitors who access or attend University premises or use University facilities, including contractors and members of the public.

(4) This policy is subject to relevant State, Territory and Commonwealth law and University rules as identified under References.

References

(5) This policy aims to be consistent with, and is to be read in conjunction with the following:

- a. [Charles Sturt University By-law 2005](#)
- b. [Charles Sturt University Act 1989 No 76](#)
- c. [Inclosed Lands Protection Act 1901 No 33](#)
- d. [Inclosed Lands Protection Regulation 2018](#)
- e. [Security Industry Act 1997 No 157](#)
- f. [Security Industry Regulation 2016](#)
- g. [Animals on University Premises Policy](#)

- h. [Code of Conduct](#)
- i. [Critical Incident Management Guidelines](#)
- j. [Emergency Management Policy](#)
- k. [Student Misconduct Rule 2020](#)
- l. [Space Management Policy](#)
- m. [Workplace Surveillance Act 2005](#)
- n. relevant standard operating procedures associated with this policy which are incorporated into instructions and training materials made available to Authorised Access Officers
- o. [Charles Sturt University Enterprise Agreement](#)
- p. [Work Health and Safety Act 2011 No 10](#)

Section 2 - Glossary

(6) For the purpose of this policy unless otherwise indicated:

- a. Access control devices - means any method for controlling access used to define and control spaces (controlled areas) to which access restrictions apply including:
 - i. electronic code-pads
 - ii. card readers and other Radio Frequency Identification Devices (RFID)
 - iii. proximity cards or key-ring fob devices
 - iv. remote arming stations
 - v. passive infra-red detectors
 - vi. duress buttons
 - vii. reed switches
 - viii. mechanical barriers
 - ix. locks and keys
 - x. university identification cards
 - xi. signs
 - xii. border definitions and instructions.
- b. Access coordinator - means persons assigned responsibility for the management of access control devices by the relevant authorised access officer.
- c. Alarm system - means any electronic intruder detection, hold-up or duress alarm system installed for the purpose of detecting or signaling security related incidents.
- d. Authorised access officer - means a staff member or University security contractor appointed in writing by the Vice-Chancellor or nominated delegates to exercise the responsibilities set out in Part C - Responsibilities:
 - i. the Vice-Chancellor
 - ii. the Chief Operating Officer
 - iii. Executive Director, Division of Facilities Management
 - iv. Director, Operational Services, Division of Facilities Management
 - v. Northern Operations Manager, Division of Facilities Management
 - vi. Southern Operations Manager, Division of Facilities Management
 - vii. Campus Facilities Managers, Division of Facilities Management
 - viii. Operations Coordinators, Division of Facilities Management
 - ix. Maintenance Coordinators, Division of Facilities Management
 - x. Maintenance and Operations Coordinators, Division of Facilities Management

- xi. Director, Uni Life, Division of Student Success
 - xii. Campus Security Officer
 - xiii. senior members of staff appointed by the Vice-Chancellor for the purpose of this policy, and
 - xiv. any person appointed as an authorised access officer in accordance with Part C of this policy.
- e. Authorised CCTV Operator - means a person authorised by the Director, Operational Services, Division of Facilities Management (or delegate) to view Closed Circuit Television System (CCTV) images or footage, live or recorded, for security, safety and/ or access purposes.
 - f. Campus security personnel - means any person engaged by the University to provide security services or traffic control functions in relation to University premises.
 - g. Card - for the purposes of this policy the word 'card' may be extended to include codes or personal identification numbers (PIN) used for access purposes.
 - h. Closed circuit television system (CCTV) includes any combination of cameras, lenses, video/digital recorders and/or accessories installed for the purpose of monitoring and/or recording visual activity that complies with the Division of Facilities Management CCTV design and installation specification.
 - i. Controlled area - means any area or space on University premises to which general or public access is not available at any designated time.
 - j. Critical assets - means any University equipment, infrastructure, documents or intellectual property, the loss of which would seriously impact on the activities of the University.
 - k. External visiting speaker - means any visitor who is not an invited visiting speaker and for whom permission is sought to speak on University premises or using University facilities.
 - l. Head contractor/principal contractor - is a person or entity that has the management or control of defined construction workplace as defined under the [Work Health and Safety Act 2011 No 10](#).
 - m. Invited visiting speaker - means any person who has been invited by the University to speak on University premises or using University facilities where, for the purposes of this definition, the 'University' includes its decision-making organs and officers; its student representative bodies, undergraduate and post-graduate; any official clubs, societies and associations recognised by the University's decision-making organs and officers or student representative bodies; and any entities controlled by the University.
 - n. Monitored alarm system - means an alarm system which is connected via LAN, WAN, PSTN, cable, radio transceiver or other means to a central monitoring station, University security control room, automatic SMS, voice message or visual alarm forwarding system which will communicate system alerts and facilitate appropriate responses to alarms.
 - o. Security - means the security office of each campus and any Campus Security Officer, Manager or Security Officer.
 - p. Security incident - means any situation arising that may compromise the security of people, assets or property on University premises, for example; acts of violence; theft or damage; suspicious or threatening behaviour; activation of any alarm; any instance of unauthorised access; disorderly or unlawful conduct, and any emergency situation such as fire, flood or accident.
 - q. Security licence - means an appropriate licence granted under the [Security Industry Act 1997 No 157](#) or the [Security Industry Regulation 2016](#) or equivalent legislation in any other relevant jurisdiction.
 - r. Security management - means the Campus Facilities Manager, Northern Operations Manager, Southern Operations Manager and the Director, Operational Services within the Division of Facilities Management, who are employed by the University to manage security operations and Security.
 - s. Supervising Staff Member - means every member of staff responsible for the provision of teaching or supervision of students, staff, contractors or visitors to the University.
 - t. University identification card - means an official photographic identity card issued by Student Central, which may, or may not, additionally function as an access control device.
 - u. University premises - means any land which is owned, controlled, managed or occupied by the University

together with any building, construction or facility of any kind, whether permanent or temporary, on that land and also includes any other building, construction or facility which is under the control or management of, or which is occupied by the University. This excludes any building sites under the control of a Head Contractor.

- v. University rules - means the [Charles Sturt University Act 1989 No 76](#), [Charles Sturt University By-law 2005](#), rules, regulations, policies, guidelines, and procedures, applying to students, staff, and visitors.
- w. Visitor - means any person who is not a University student or member of staff but who accesses or speaks on University premises or using University facilities, including contractors to the University and members of the public.

Section 3 - Policy

Part A - Access to and use of University premises

(7) Persons with a valid reason may access and use University premises (including University facilities), provided that:

- a. access or entry has not been prohibited by any authorised access officer,
- b. in the case of a visitor who wishes to speak on University premises or using University facilities for an event not directly related to core teaching or research activities, permission has been granted in accordance with this policy, and
- c. they comply with any relevant policies, procedures and/or terms and conditions imposed on or applicable to their right of access to and use of the University premises or facilities.

(8) All staff and students and applicable contractors are issued with University identification cards which must be:

- a. carried during attendance on University premises, and
- b. shown in response to any reasonable request from any authorised access officer or any other member of staff who might require such identification in the course of their duties.

Incidents and emergencies

(9) This policy does not limit the right of any State, Territory or Federal Police Officer to access University premises and/or to take action consistent with their relevant authorities and powers, either in an emergency situation or as part of their general services to the public.

(10) Emergency Services may, from time to time, conduct specific operations on University premises.

(11) Any member of Security who calls the Emergency Services to University premises must immediately inform a member of Security Management. Depending upon the nature of the event, the Chief Warden may enact the [Critical Incident Management Guidelines](#).

(12) In the event of the Emergency Services being called to attend an emergency on University premises by any staff, student or visitor, the person instigating the call must inform a member of Security as soon as possible advising the nature of the emergency to allow Security to coordinate and expedite Emergency Services attendance.

(13) A head contractor in control of a building site is required to have emergency arrangements in place.

Visitors who speak on University premises or using University facilities

(14) The University has the right and responsibility to determine the terms and conditions upon which it permits visitors to speak on University premises and using University facilities.

(15) Any person who wishes to invite a visitor to speak on University premises or using University facilities for an event not directly related to core teaching or research activities should seek the written permission of an authorised access officer. The authorised access officer may:

- a. require any person or persons organising the event to comply with the University's booking procedures and to provide information relevant to the conduct of the event (including any proposed or likely topic or content of any speech) and any public safety and security issues,
- b. distinguish between invited visiting speakers and external visiting speakers in framing any requirements or conditions,
- c. refuse permission to any visitor to speak on University premises or use University facilities where the content of the speech is or is likely to:
 - i. be unlawful,
 - ii. prejudice the fulfilment by the University of its duty to foster the wellbeing of staff and students, including if the speech is or is likely to breach the University's [Harassment and Bullying Prevention Policy](#) or [guidelines](#),
 - iii. involve the advancement of theories or propositions which purport to be based on scholarship or research but which fall below scholarly standards to such an extent as to be detrimental to the University's character as an institution of higher learning,
- d. require that any person or persons seeking permission for the use of the University's premises or facilities for any external visiting speaker to contribute in whole or in part to the cost of providing security and other measures in the interests of public safety and order in connection with the event at which the external visiting speaker is to speak.

(16) Subject to this policy and other University rules, policies and procedures, the University will not limit the right to free speech or refuse permission for the use of University premises or facilities by a visiting speaker nor attach conditions to its permission, solely on the basis of the proposed or likely topic or content of the proposed speech by the visiting speaker.

Controlled areas

(17) An authorised access officer may designate a controlled area to regulate access within University premises to ensure the security and safety of people and university property.

(18) Controlled areas are identified by:

- a. signs,
- b. locked doors,
- c. fences,
- d. boom-gates,
- e. barrier tape, or
- f. defined by the instruction of campus Security personnel or an authorised member of staff.

(19) Persons must not access a controlled area without approval by an authorised access officer.

Access control devices

(20) Access control devices are issued by the University to allow students, staff, and approved visitors access to controlled areas of the University. These must be used in accordance with any accompanying instructions and shall:

- a. not be interfered with under any circumstances,

- b. only be used to access controlled areas for which they are currently authorised,
- c. only be used by the person to whom they have been issued - they must not be lent, given to or used by any other person to access a controlled area for which they have no authorised right of access, and
- d. remain the property of the University and must be returned on demand at any time.

(21) Unauthorised possession, use or tampering of an access control device by staff or students, shall be deemed to have committed a breach of discipline or misconduct under the relevant University policy, in particular, the Staff [Code of Conduct](#) and [Student Misconduct Rule 2020](#).

(22) The selection, installation, maintenance and operation of all access control devices and associated equipment at University premises must be made in consultation with, and seek final approval from the Division of Facilities Management.

(23) To ensure compliance with applicable fire and building safety codes, non-university approved access control equipment, including mechanical keys or locks, must not be used.

(24) Any unauthorised fabrication, duplication, issuing, possession, or use of access control devices is strictly prohibited. Fabrication of any access control devices must only be performed after written approval from the Division of Facilities Management.

Monitoring access and safety

CCTV

(25) The primary use of CCTV is to discourage unlawful behaviour and to assist in the successful prosecution of individuals involved in unlawful behaviour in and around University premises.

(26) Only CCTV equipment that meets the Division of Facilities Management's Operational Design Standards shall be applied to University premises.

(27) Appropriate standard operating procedures shall be applied to all security CCTV applications to ensure effective and ethical management of equipment. Recorded information is appropriately maintained and accessed by authorised CCTV operators. All security CCTV systems installed will comply with the following:

- a. located in a secure area,
- b. signage installed in accordance with the legislation of the relevant State or Territory,
- c. access to CCTV controllers and recorders shall be limited to authorised CCTV operators only,
- d. all security CCTV equipment shall be integrated into the University's wider electronic Security and Access Control System to enable effective monitoring by Security, and
- e. used in accordance with any relevant legislation or applicable codes of practice.

Alarm systems

(28) The Division of Facilities Management has responsibility for selection, installation and maintenance of all alarm systems on University premises.

(29) University property containing critical assets, highly confidential or sensitive information will be considered for protection by a suitable monitored alarm system.

(30) Staff performing tasks which may be accompanied with a higher than usual security related risk may (as part of an overall security solution) be considered for protection by a suitable monitored alarm system, such as a personal duress alarm.

(31) All staff, students and visitors are responsible for considering their own environmental security issues and are encouraged to seek professional advice from the Division of Facilities Management regarding the most appropriate security solutions. This may include alarm systems such as personal duress alarms.

Part B - Disorderly conduct

(32) Disorderly conduct is recognised as general misconduct and subject to relevant University Rules governing misconduct, for example, the [Charles Sturt University Enterprise Agreement](#), [Student Misconduct Rule 2020](#) and the [Code of Conduct](#).

(33) Disorderly conduct includes the following forms of conduct and may lead to action being taken by authorised access officers:

- a. failure to comply with University rules,
- b. conduct which impairs the reasonable freedom of other persons to pursue their studies, research, duties or lawful activities in the University or to participate in the life of the University,
- c. threatening the health, safety or welfare of staff, students or visitors of the University,
- d. willfully failing to obey any reasonable direction of authorised access officers in relation to University premises (including University facilities), access and/or conduct or order,
- e. failing to provide appropriate identification on request by an authorised access officer,
- f. willfully accessing any place on University premises which the person is forbidden to access,
- g. willfully littering, damaging, defacing, or wrongfully dealing with any university property or any other property on University premises, and
- h. any other unreasonable conduct disrupting the normal activities of the University.

Reporting disorderly conduct

(34) In the occurrence of an alleged act of disorderly conduct which poses a threat or risk to personal safety, or which requires immediate intervention; staff, students and visitors must contact Police and Security immediately.

(35) Complaints reported to Security alleging disorderly conduct by students must be reported to the Manager, Student Conduct by Security as soon as practicable after the alleged misconduct has occurred.

(36) Complaints regarding alleged disorderly conduct by staff that requires Security intervention must be reported to the Division of People and Culture as soon as practicable after the alleged misconduct has occurred by Security.

(37) Complaints regarding alleged disorderly conduct against visitors must be reported to Security. Security shall notify the Manager, Student Conduct as soon as practicable after the alleged misconduct has occurred.

Part C - Responsibilities

Security incidents

(38) All security incidents which occur on University premises must be reported to Security.

(39) Security is responsible for ensuring Police are notified of all incidents on University premises where appropriate, including those relating to the loss or damage of university property.

(40) It is the responsibility of any individual who has suffered loss or damage to personal property to notify Police and Security. Once notified, Security will attend the site and complete a University Security Incident Report.

Division of Facilities Management

(41) Division of Facilities Management are responsible for the administration of access to University premises including:

- a. maintaining the security and safety of University premises,
- b. providing access to common areas, such as learning commons and timetabled teaching spaces,
- c. managing the University's access control systems which provide access to controlled areas,
- d. promoting uniformity and compatibility of access control devices used at University premises and for the maintenance of central records, and
- e. providing adequate training for access coordinators.

Security staff

(42) The role of Security staff is to provide staff, students and visitors with a safe and secure environment which facilitates and promotes learning, teaching and research.

(43) Security staff will fulfill their duties in a lawful, fair and equitable manner without damage to the University's reputation or unfairly impinging on the rights of individuals.

(44) Security staff will take reasonable action to assist with:

- a. maintaining public order on University premises,
- b. the prevention and investigation of crimes against an individual on University premises and report suspected crimes to the Campus Facilities Manager, Division of Facilities Management, the Police and other relevant external authorities. Crimes such as:
 - i. assaults,
 - ii. offensive behaviour,
 - iii. indecent exposure, or
 - iv. trespass etc.
- c. the prevention and investigation of property crimes on University premises and report suspected crimes to the Campus Facilities Manager, Division of Facilities Management, the Police and other relevant external authorities. Crimes such as:
 - i. willful damage,
 - ii. theft, and
 - iii. burglary.
- d. managing emergencies and critical incidents, including reporting emergencies to the Campus Facilities Manager, Division of Facilities Management, Police, Fire, Ambulance and other relevant external authorities. Emergencies such as:
 - i. fires,
 - ii. chemical spills, and
 - iii. injuries.
- e. providing information and assistance to the public in the circumstance where Security are the first and possibly only available contact for the University, and
- f. ensuring staff, students and visitors comply with the law and University rules whilst on University premises.

Security Master License

(45) The [Security Industry Act 1997 No 157](#) requires the University to maintain a current Security Master

Licence where it directly employs staff as Campus Security Officers to carry out security activities as defined under the Act. The responsible officer for the University's Security Master Licence is the only person who can authorise the employment of Campus Security Officers.

(46) Under no circumstances shall any persons be employed or engaged by the University as a member of Security without the written consent of the Security Master Licence holder, Director, Operational Services, Division of Facilities Management.

Authorised access officers

(47) Authorised access officers are invested with the authority to make enquiries and take reasonable action, in compliance with this policy and associated documentation, to regulate the access and behaviour of staff, students and visitors. This includes:

- a. requesting any person on University premises to produce proof of identity,
- b. considering requests and setting terms and conditions that apply to visitors who wish to speak on University premises or using University facilities,
- c. making reasonable and necessary enquiries to validate an individual's status if they are unable to produce their university identification card or otherwise justify their right to be on University premises,
- d. requesting any staff, student or visitor to leave University premises and/or to cease using University facilities if:
 - i. they are unable to produce appropriate identification or justification for being on University premises or to use University facilities,
 - ii. the authorised access officer has reasonable grounds to believe that the person has committed, is committing or is about to commit a criminal act, or breach University rules,
 - iii. the person is involved in disorderly conduct (see Part B Disorderly Conduct), or
 - iv. the person is acting in a way that may threaten public order, damage property or otherwise pose a threat to the safety and wellbeing of staff, students or visitors on University premises or on or within University facilities.

(48) Authorised access officers are invested with the authority to administer and control vehicle access to University premises and the traffic and parking provisions therein.

(49) Authorised access officers are responsible for appointing access coordinators for their area of responsibility.

(50) Authorised access officers will call Police for assistance where any person refuses to comply with a request to leave the University premises and may take any other actions they consider reasonably appropriate with respect to any person who refuses to comply with the terms and conditions of use of University premises or University facilities.

(51) It is expected that all authorised access officers are fully conversant with relevant standard operating procedures prior to commencing duties at the University and throughout their employment.

(52) Authorised access officers must have their University identification card or security licence prominently displayed at all times or be able to produce this on demand.

Access coordinators

(53) Access coordinators are appointed by the relevant authorised access officer and have authority to grant, deny or revoke access privileges to controlled areas for which the faculty, division or centre is directly responsible.

(54) Access coordinators are responsible for:

- a. managing access control devices within their allocated space in accordance with this policy, and

- b. managing internal access within the allocated space, as per the [Space Management Policy](#) under the direction of the access coordinator's senior manager.

Supervising staff members

(55) Supervising staff members are responsible for those under their control. This may include other staff, visitors (including contractors) or students.

(56) Supervising staff members are responsible for ensuring approved persons are inducted and supervised into controlled areas. They must also provide instruction and supervision at a level that maintains the security of the area, safety of staff, students and visitors; and protection of University property.

(57) Supervising staff members who witness disorderly conduct by students, staff, visitors (including contractors) on or using University premises, must:

- a. request the individual(s) to discontinue the disorderly conduct,
- b. request the individual(s) to leave the area and/or cease using the facilities,
- c. contact the Police and Security for further assistance if the individual(s) refuse to comply, and
- d. report each incident in accordance Part B - Disorderly Conduct.

Section 4 - Procedures

(58) Nil.

Section 5 - Guidelines

(59) Nil.

Status and Details

Status	Current
Effective Date	4th December 2020
Review Date	20th July 2023
Approval Authority	Chief Operating Officer
Approval Date	4th December 2020
Expiry Date	Not Applicable
Unit Head	Nicholas Mamouzelos Chief Security Officer
Author	Nicholas Mamouzelos
Enquiries Contact	Division of Facilities Management +61 2 69332286

Glossary Terms and Definitions

"Duty to foster the wellbeing of staff and students" - includes the duty to ensure that no member of staff and no student suffers unfair disadvantage or unfair adverse discrimination on any basis recognised at law including race, gender, sexuality, religion and political belief; includes the duty to ensure that no member of staff and no student is subject to threatening or intimidating behaviour by another person or persons on account of anything they have said or proposed to say in exercising their freedom of speech; supports reasonable and proportionate measures to prevent any person from using lawful speech which a reasonable person would regard, in the circumstances, as likely to humiliate or intimidate other persons and which is intended to have either or both of those effects; does not extend to a duty to protect any person from feeling offended or shocked or insulted by the lawful speech of another.