Surveillance Procedure

Section 1 - Purpose

(1) This procedure:

a. notifies workers, students and other entrants to University premises or users of University resources of the circumstances and types of surveillance conducted by Charles Sturt University (the University)
b. supports compliance with the Workplace Surveillance Act 2005 (NSW), which regulates surveillance of workers in the workplace.

Scope

(2) This procedure applies to:

a. all workers, students, and entrants to any University premises
b. users of University managed information and communication technology (ICT)
c. any persons at any place while performing work for the University, using equipment or systems provided by or at the expense of the University, including ICT resources and networks.

Section 2 - Policy

(3) This procedure supports the Privacy Management Plan, as well as activities authorised under the Facilities and Premises Policy and the Information Technology Policy.

Section 3 - Procedure

Surveillance conducted by the University

(4) The University carries out surveillance to:

a. protect the health, safety and welfare of workers, students and other entrants to University premises
b. protect the personal information and privacy of workers, students and others
c. secure its facilities and resources against theft, fraud, malicious or accidental damage and other security breaches
d. maintain the integrity, security and continuity of its ICT resources.

(5) The University conducts surveillance in ways set out in the table at clause 6. The University does not use surveillance to proactively track the location or activities of individuals unless approved by a delegated officer to lawfully do so. However, the University may use the surveillance information and surveillance records captured as set out under the 'Access and use etc' heading of this procedure.

Types of surveillance

(6) The types of surveillance used by the University are:

Camera surveillance	The University uses security cameras to monitor or record visual images of activities on its premises on an ongoing and continuous basis.	1. Clearly visible, fixed security cameras (including camera casings or other equipment that indicates the presence of a camera) are installed throughout University managed campuses, in internal and external locations. The University does not use covered or hidden security cameras. 2. The University does not use security cameras in bathrooms, change rooms, parents' rooms or bedrooms. 3. Signs notifying people of the presence of cameras will be clearly visible at entrances to locations. 4. Installation of security cameras/CCTV is managed in accordance with the Facilities and Premises Policy and Facilities and Premises Procedure - Access, Use and Security.
Computer surveillance	The University monitors the use of its ICT systems and environment on an ongoing and continuous basis.	1. Computer surveillance includes monitoring: 1. University email accounts and emails sent or received using a University email account or a University server 2. University collaborative, recording and communication tools (e.g. Teams, Zoom) 3. internet usage, including browsing history, content downloads and uploads, video and audio file access, and any data input using the ICT resources 4. the use of USB ports and attached storage devices and other peripherals; and data that is uploaded from or downloaded to attached devices 5. the logon and access location of University issued devices 6. access (including logons) to, and all activity on, the ICT resources including computer hard drives and servers, and any files stored on ICT resources. 2. Use of University ICT resources is subject to the Information Technology Policy and Information Technology Procedure - Acceptable Use and Access.
Tracking surveillance	The University provides, and makes available for use by workers, equipment and devices that have the active functionality to monitor and record their geographical location or movement. Location data may be monitored temporarily or for specific periods, in accordance with this procedure and the Workplace Surveillance Act.	1. This includes: 1. mobile telephones, hand-held radios, laptops, tablets and similar devices 2. access cards and credentials into University buildings 3. University-owned vehicles with global positioning systems installed (all such vehicles have a notice on them indicating that the vehicle may be subject to tracking surveillance) 4. fuel cards issued for University-owned vehicles 5. wired and wireless data point connections installed in University buildings.

(7) The conduct of any surveillance in addition to that set out at clause 6 must be approved by the Vice-Chancellor and permissible under the Workplace Surveillance Act.

Notification

(8) The University notifies people about the surveillance it conducts in the following ways:

a. Publicly available policies and procedures, including the Facilities and Premises Procedure - Access, Use and Security, Information Technology Procedure - Acceptable Use and Access and this procedure.

b. For surveillance cameras, by means of physical signage at the entrances to or within campus grounds, and on campus plans in FMCentral.
c. For computer surveillance, by obtaining acknowledgement and agreement to adhere to the Information Technology Policy/Information Technology Procedure - Acceptable Use and Access when an authorised user activates their University account or updates their password.
d. For employees, by obtaining a signed acknowledgement when an employee commences employment and regular (usually annual) reminder notifications.
e. University workers will be given at least 14 days written notice before any additional or new surveillance is undertaken by the University, except where a covert surveillance authority is obtained. See also the 'Covert surveillance' heading in this procedure.

Surveillance information and records

(9) The University creates and stores the following surveillance information and surveillance records:

a. Movements of persons within University facilities and premises, including workspaces and student residences.
b. Access to secure University facilities.
c. Connection of devices (whether or not owned by the University) to ICT resources, including logging access at specified wired and wireless data points.
d. Emails sent or received using University email accounts or through University servers, storage volumes, download volumes, browsing or upload and download history on ICT resources.
e. Any information or data created or managed on, downloaded to and stored on ICT resources, that the University manages, supplies or otherwise makes available for use.

(10) Surveillance information and records are captured, stored and retained in accordance with the Privacy Management Plan, Records Management Policy and Information Security Guidelines.

Access to and use of surveillance information and records by the University

(11) The University may use or disclose surveillance information or surveillance records in accordance with the Privacy Management Plan, Information Technology Procedure - Acceptable Use and Access and the Workplace Surveillance Act. This may include the following:

a. For the legitimate business purposes related to the object and functions of the University, including the provision of learning and teaching, employment of staff, research, trend analysis and continuous improvement purposes.
b. Internal inquiries and investigations of alleged unlawful activities or activities that are alleged to be in breach of any University rule, policy or code of conduct or in breach of a person's duties to the University.
c. For use or disclosure in civil or criminal legal proceedings to which the University is a party or is directly involved.
d. Disclosure to a member or officer of a law enforcement agency, Independent Commission Against Corruption, NSW Ombudsman or safety regulator for use in connection with the detection, investigation or prosecution of an offence.
e. Where it is reasonably necessary to avert an imminent threat of serious violence to a person or substantial damage to property (which may include disruption to the University's business, network, ICT resources, systems or operations).
f. Where otherwise required or authorised by law to do so (for example, compliance with a search warrant or subpoena, or in response to a GIPA application).

(12) Access to surveillance information and surveillance records is restricted to the following:

a. Employees whose normal duties include routine backup or restoration of data, conduct of audits, review of web filtering, email filtering, document retrieval or logs, or other activities relating to the University's systems, including ICT resources, cyber security and networks.
b. Employees whose normal duties include review of camera footage and of building access (including use of building access devices).
c. Persons whose access is approved by the Executive Director, Safety, Security and Wellbeing or the Director, Security and Resilience (CSO).

Prohibited surveillance

(13) The University will not carry out any types of surveillance which are prohibited under Part 3 of the Workplace Surveillance Act:

a. Surveillance of persons in a change room, toilet facility or shower or other bathing facility.
b. Surveillance of workers using work surveillance devices when not on University premises or performing work for the University, with the exception of computer surveillance when using ICT resources provided by or at the expense of the University, or as otherwise permitted under the Workplace Surveillance Act.
c. Preventing or blocking emails or internet access of any authorised user except as permitted under the Workplace Surveillance Act s 17, and/or in accordance with the Information Technology Procedure - Acceptable Use and Access, this procedure, or other University policy. The University is not obliged to notify a worker that it has prevented delivery of an email if:
    i. the email was a commercial electronic message, within the meaning of the Spam Act 2003 (Cth)
    ii. the content or attachments of the email would or might result in unauthorised interference with, damage to or operations of a network or ICT resource (including any program run or data stored on any ICT resource)
    iii. the University regards the content of the email, including any attachment(s), as menacing, harassing or offensive
    iv. the sender of the email has been identified as having previously sent malicious content to the organisation
    v. the University is not aware (and cannot reasonably be expected to be aware) of whether a worker has sent that email or of the identity of the employee who has sent that email.

Covert surveillance

(14) The University will not carry out covert surveillance of its workers (that is, any surveillance that has not been notified by this procedure or is otherwise noncompliant with Part 2 of the Workplace Surveillance Act) unless a covert surveillance authority has been issued by a Magistrate under Part 4 of that Act.

Section 4 - Guidelines

(15) Nil.

Section 5 - Glossary

(16) For the purpose of this procedure:

a. Authorised user – see the Information Technology Policy.
b. ICT resources – see the Information Technology Policy.

c. Surveillance (of a worker) – means surveillance of a worker by any of the means referred to in clause 6 of this procedure.
d. Surveillance information – means information obtained, recorded, monitored or observed as a consequence of the surveillance carried out by the University.
e. Surveillance record - means a record or report of surveillance information.
f. Worker – means current University employees, contractors, consultants, adjuncts, conjoints or volunteers who have access to any University premises, equipment, or systems, including network or ICT resources.
g. Workplace – means any University premises or any other place where workers perform work for the University, or any part of such premises or place.

Status and Details

Status	Current
Effective Date	27th September 2023
Review Date	27th September 2026
Approval Authority	Chief Operating Officer
Approval Date	27th September 2023
Expiry Date	Not Applicable
Unit Head	Stacey Jenkins Executive Director, Safety, Security and Wellbeing
Author	Frank Tamsitt Chief Security Officer
Enquiries Contact	Division of Safety, Security and Wellbeing