Surveillance and Location Tracking procedure

Section 1 - Preamble

(1) This Procedure is effective from 26 July 2022.

Section 2 - Purpose

(2) This Procedure governs the University's approach to the use of surveillance and location tracking in its operations.

Section 3 - Scope

(3) This Procedure applies to all staff, students and associates of the University.

Section 4 - Policy

(4) This Procedure is pursuant to the Privacy policy.

Section 5 - Procedure

(5) Deakin seeks to provide a safe and secure environment for its students, staff, associates and visitors to its premises.

(6) For these purposes, and subject to clause 7, the University may collect and use personal information through use of surveillance devices:

a. where necessary
    i. to protect people, property and facilities from harm, damage or loss;
    ii. to prevent and deter unlawful activity and breaches of the University's regulations, policies and procedures;
    iii. to investigate and prosecute illegal and unlawful activity and manage breaches of the University's regulations, policies and procedures;
    iv. to provide and monitor access to buildings and secure facilities;
    v. to analyse pedestrian and vehicle movement across its campuses and inside buildings;
    vi. to provide information needed for emergency management;
b. where incidental to the operation of the campuses; and
c. where authorised or required by law.

(7) Drones must not be used or permitted on the University's premises without prior written approval of the Privacy

Officer.

(8) Personal information collected by surveillance devices will be retained only for so long as it is necessary for the purpose of collection and must be disposed of in accordance with the retention schedules maintained under the Information and Records Management procedure or, in the case of CCTV footage, as provided in clause 27.

Installation and Positioning of CCTV Cameras

(9) The installation of a CCTV camera or system on Deakin property must comply with legal requirements and University policy.

(10) CCTV cameras that capture or record an individual's image:

a. must not be installed in toilet facilities, restrooms, changerooms, rooms designated for breastfeeding or rooms designated for prayer, except where required by law.
b. directed at windows of rooms in a manner that allows an individual to be identified if an individual in that room would have a reasonable expectation of privacy. An example is a residence room.

(11) Dummy CCTV cameras must not be used as part of a surveillance system as these give stakeholders a false sense of security.

(12) Staff, students and visitors should not expect that CCTV monitors are continuously monitored in real time.

(13) The Manger, Security Operations must ensure that appropriate signs are placed at all entry points to a building or secure access facility where CCTV cameras will be operating.

Use and Disclosure of Personal Information Collected via CCTV

(14) The University will use personal information collected via CCTV to the extent necessary to meet the objectives set out in clause 6.

(15) Personal information collected via CCTV will not be made available for research purposes, to monitor attendance at events, or to promote the University.

(16) The General Counsel must approve all disclosure of footage and images collected via CCTV, whether by provision of a copy of footage or images or by permitting a third party to review footage or images.

(17) Requests for access to or disclosure of footage and images collected via CCTV for the purposes of non-criminal investigations, litigation or administrative proceedings must be referred to the General Counsel, who will manage all disclosures and communication relating to the request.

(18) In the case of a request from a law enforcement agency to view or obtain a copy of CCTV footage or images captured by CCTV, the request must be provided to the General Counsel for review, together with a copy of the footage or image sought. The General Counsel will determine if the footage or image should be disclosed by the Manager, Security Operations and under what conditions, which may include blurring or redaction of personal information appearing in the footage or image.

(19) If the General Counsel authorises disclosure of a copy of the CCTV footage or image, the Manager, Sceurity Operations will provide the General Counsel with a duplicate copy of the CCTV footage or image as disclosed.

(20) Footage or images disclosed on personal storage devices or transmitted electronically must be encrypted.

Security of CCTV Footage and Images

(21) CCTV footage and images captured by CCTV must be protected from inadvertent or unauthorised access and disclosure. The Manager, Security Operations must ensure that CCTV monitors are located in a secure area accessible only by Authorised Users and where they are not visible to third parties.

(22) Authorised Users must be trained in the use of CCTV and must have privacy training.

(23) No Authorised User may copy or modify any CCTV footage or image without prior written authorisation of the Privacy Officer.

(24) No Authorised User may distribute, forward, broadcast, live stream, transmit or publish in any form or media any CCTV footage or image or permit any third party to do so.

(25) CCTV footage will be kept for a period of 30 days, after which it will be securely overwritten unless it is identified as needed further for an investigation, prosecution or proceeding.

(26) If CCTV footage is needed for further investigation, prosecution or proceeding, it must be securely stored separately from the CCTV system so that it is not overwritten.

(27) CCTV footage stored under clause 26 must not be destroyed without the authorisation of the Information Manager, Information and Records Services.

(28) Passwords may not be shared among Authorised Users and a generic password used by all authorised users must not be used.

(29) Audit logs of access to and disclosure of CCTV footage and images must be maintained to enable the University to assure compliance with this Procedure.

Location Tracking

(30) The University may identify the location of a mobile device when it is connected to Eduroam or other technology at its campuses, corporate centres, regional learning centres or other facilities where the University carries out its activities.

(31) The University may collect and use location data from mobile devices

a. to provide wayfinding services;
b. to provide information targeted to a specific location;
c. to assist in room allocation and planning;
d. to analyse and improve traffic flow across campuses and inside buildings;
e. to provide emergency information and assistance;
f. where authorised or required by law.

(32) The University may identify the location of an individual communicating with the University or a service provider to the University from the IP address from which the individual communicates.

(33) The University may combine location data with other data held by the University

a. where necessary to locate an individual during an emergency or threat to public health and safety, or
b. to investigate breaches of academic or research integrity (an example is in the use of on-line invigilation tools); or
c. as otherwise required by law.

(34) If a law enforcement agency seeks to view or obtain a copy of location data held by the University, the request must be provided to the Privacy Officer for review, together with particulars of the data held. The Privacy Officer will consult with the General Counsel to determine if the location data should be disclosed and under what conditions and will manage all communications and disclosure relating to the request.

(35) Location data will be retained only for so long as it is necessary for the purpose of collection and must be disposed of in accordance with the retention schedules maintained under the Information and Records Management procedure.

Access

(36) Individuals are entitled to access their personal information collected via surveillance devices and their location data, where personally identifiable, collected by the University. Access is managed in accordance with the Privacy policy. The University will provide access in a manner that protects the privacy of other persons captured in the footage or image

Section 6 - Definitions

(37) For the purpose of this Procedure:

a. associates: contractors, consultants, volunteers, visiting appointees and visitors to the University.
b. Authorised User: the Manager, Security Operations and Deakin staff members designated by the Manager, Security Operations to have access to CCTV system.
c. CCTV (Closed Circuit Television): a system that transmits images on a 'closed loop' basis, where images are only available to authorised users for monitoring in real time or are recorded for later review.
d. location tracking: use of data collected from an individual's computer or mobile device to identify the device's physical location.
e. law enforcement agency: as defined in the Privacy and Data Protection Act 2014 (Vic)
f. Privacy Officer: the staff member (or their delegate) appointed under the Privacy policy, who may be contacted at privacy@deakin.edu.au.
g. surveillance devices: technology capable of being used to observe, monitor, record or locate an individual, a group of individuals, an object or a place/location, including CCTV, drones and vehicle licence plate capture. It does not apply to live streaming or other technology used in the delivery of Deakin units, conferences or other presentations.

Status and Details

Status	Current
Effective Date	26th July 2022
Review Date	26th July 2023
Approval Authority	Vice-Chancellor
Approval Date	25th July 2022
Expiry Date	To Be Advised
Responsible Executive	Kerrie Parker Executive Vice-President Resources evpr@deakin.edu.au
Implementation Officer	Shirley Rooney General Counsel +61 3 52278560
Enquiries Contact	Shirley Rooney General Counsel +61 3 52278560