

Workplace Surveillance Policy

Section 1 - Purpose

(1) This Policy establishes the types of Workplace Surveillance that may be undertaken at Macquarie University (the University) and how such surveillance may be undertaken.

Background

(2) This Policy is intended to meet the requirements of the [Workplace Surveillance Act 2005](#). Publication of this Policy constitutes written notice to all workers regarding workplace surveillance undertaken by the University.

Scope

(3) This Policy applies to all workers of the University while at work.

Section 2 - Policy

Part A - Notification

(4) The University may, to the extent permitted by law, conduct camera, computer, and/or tracking workplace surveillance of workers while at work.

(5) From the commencement of a worker's employment or engagement, and on an intermittent and/or continuous, ongoing basis, the University may conduct workplace surveillance by:

- a. accessing, monitoring, logging and recording any communication or information developed, used, received, stored or transmitted by a Worker using the University's IT Systems (either at the University or at any other place and including a Worker's private use of the University's IT Systems);
- b. installing filtering systems in the University's IT Systems which restrict the inward and outward flow of certain types of material, including emails and viruses, with the result that some email traffic may be blocked;
- c. conducting camera surveillance of workers at work for the purpose of physical and IT security risk management; and
- d. conducting tracking surveillance by means of an electronic device, the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device).

(6) Any such workplace surveillance will be in accordance with the provisions of the [Workplace Surveillance Act 2005](#).

Part B - Additional Restrictions on Camera Surveillance and Tracking

(7) Cameras will be visible and a sign notifying workers that they may be under surveillance will be visible in the areas in which cameras operate.

(8) Tracking surveillance will only be carried out where notice is clearly on the vehicle or other thing indicating that the vehicle or thing is the subject of tracking surveillance.

Part C - Use and Disclosure of Surveillance Records

(9) The University may use or disclose any surveillance record where it has a reasonable basis, unless otherwise prohibited by law. The following will constitute a reasonable basis to use or disclose a surveillance record, but is not intended to constitute an exhaustive list:

- a. ensuring security (including protecting networks or data stored on University IT Systems, and protecting the integrity of University IT Systems);
- b. using or disclosing a surveillance record in relation to a legitimate purpose related to the employment or engagement of a worker or the business activities or functions of the University;
- c. disclosure to a member or officer of a law enforcement agency (e.g. Police), Independent Commission Against Corruption or safety regulator (e.g. SafeWork NSW) for use in connection with the detection, investigation or prosecution of an offence;
- d. for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings;
- e. where it is reasonably believed to be necessary to avert an imminent threat of serious violence or of substantial damage to property; or
- f. any other reason that meets the requirements of section 18 of the [Workplace Surveillance Act 2005](#).

(10) The University will not disclose a surveillance record unless it has complied with this Policy or is otherwise permitted by applicable laws.

(11) The [Information Classification and Handling Procedure](#) sets out the requirements for accessing a surveillance record.

Part D - Covert Surveillance

(12) The University must not carry out or cause to be carried out, covert surveillance of an employee while the employee is at work, unless the surveillance is authorised by a covert surveillance authority. Any covert surveillance must be carried out in accordance with the relevant provisions of the [Workplace Surveillance Act 2005](#).

Section 3 - Procedures

(13) Nil.

Section 4 - Guidelines

(14) Nil.

Section 5 - Definitions

(15) The following definitions apply for the purpose of this Policy:

- a. At Work means when a Worker is:
 - i. at a workplace of the University (or any controlled entity of the University), including any remote working arrangements, whether or not the Worker is actually performing work at the time, or
 - ii. at any other place while performing work for the University (including if the Worker is working from remotely).
- b. Worker means any staff member of the University (or any controlled entity of the University), including officers

and employees, any contractor of the University, including any person working for a contractor, any appointees to conjoint, adjunct, emeritus, honorary, clinical, and visiting academic positions at the University and volunteers.

- c. Surveillance Record means a record or report of information obtained, recorded, monitored or observed as a consequence of Surveillance.
- d. Types of Surveillance:
 - i. Overt – used as part of a physical or IT security risk management program
 - ii. Covert – used to capture unlawful activity
- e. University IT Systems includes all electronic data, hardware, software, networks, emails and other systems owned, controlled or licenced by the University (or any controlled entity of the University), including all Information Technology Resources as defined by the [Acceptable Use of IT Resources Policy](#).
- f. Workplace means premises, or any other place, where Workers conduct work, or any part of such premises or place.
- g. Workplace Surveillance means surveillance of a Worker by any of the following means:
 - i. Camera Surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place;
 - ii. Computer Surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites or networks);
 - iii. Tracking Surveillance by means of an electronic device, the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device).

Status and Details

Status	Current
Effective Date	11th July 2022
Review Date	11th July 2025
Approval Authority	Vice-President, Professional Services
Approval Date	11th July 2022
Expiry Date	Not Applicable
Responsible Executive	David Ward Chief People Officer
Responsible Officer	David Ward Chief People Officer
Enquiries Contact	Claire Don Senior Employee Relations Consultant +61 2 9850 7471