Workplace Surveillance Policy

Section 1 - Purpose and Context

Purpose

(1) The purpose of this Policy is to describe the circumstances in which the University conducts Surveillance of its Employees.

(2) The Workplace Surveillance Act 2005 (NSW) regulates Surveillance of Employees at work by means of camera, computer, and tracking devices, and requires that Employees be notified as to the nature of that Surveillance.

(3) This Policy constitutes the provision of notice to Employees of the University's Workplace Surveillance under the Act.

Application and Compliance

(4) This Policy applies to all current Employees, contractors, consultants and University controlled entities who have access to any University premises, equipment, or systems, including IT Resources and Networks.

(5) The University may take disciplinary action, up to and including termination of employment, for any breach of this Policy.

(6) This Policy should be read in conjunction with relevant University policies, including:

a. Code of Conduct;
b. Digital Information Security Policy;
c. Email Policy;
d. Acceptable Use of Digital Services Policy;
e. Mobile Telecommunication Devices Policy;
f. Privacy Policy and Privacy Management Plan; and
g. Whistleblowing (Reporting Corruption and Other Serious Wrongdoing) Policy.

Section 2 - Definitions

(7) The Act does not separately distinguish between the terms "Surveillance" and "Monitoring", and the term "Monitoring" is defined separately in this Policy to provide clarity. However, it is still a form of "Surveillance" as defined in the Act.

(8) For the purposes of this Policy:

a. "Act" means the Workplace Surveillance Act 2005 (NSW);
b. "at work" includes where the employee is at a University Workplace whether or not they are actually performing work at the time, or at any other place while performing work for the University or utilising University resources or services;

c. "Employee" means current employees, contractors, and consultants who have access to any University premises, equipment, or systems, including IT Resources, adjuncts, conjoints and students;
d. "IT Resources" means systems, software, hardware, and other forms of technology, communication or other similar services owned or managed by the University;
e. "Malicious Content" means content of a profane or inappropriate manner including, but not limited to:
    i. pornography;
    ii. sexual content;
    iii. defamatory content;
    iv. content that harasses, threatens or bullies a person;
    v. racist content; and
    vi. violent content;
f. "Monitoring" is a form of Surveillance, and means the collection or storage of information, or the creation of records, in a routine and passive manner. It also includes routine review of that information or those records to ensure the integrity, security and service delivery of the University's systems, including IT Resources and Networks. However, and for the avoidance of doubt, Monitoring does not involve actively investigating or keeping track of an individual or their activities.
g. "Network" means network hardware and the services operating on the hardware or utilising the hardware to perform tasks, whether wired or wireless.
h. "Policy" means this Workplace Surveillance Policy and includes any Schedules or attachments;
i. "Surveillance" of an Employee means surveillance of an Employee by any of the following means:
    i. camera surveillance which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place;
    ii. computer surveillance which is 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);
    iii. tracking surveillance, which is 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);
j. "Surveillance Information" means information obtained, recorded, monitored or observed as a consequence of Surveillance of an Employee;
k. "Surveillance Record" means a record or report of Surveillance Information;
l. "University" means Western Sydney University;
m. "Workplace" means any University premises, or any other place, where employees work, or any part of such premises or place.

For the avoidance of doubt words or terms used in this Policy have the same meanings given to them in the Act.

Section 3 - Policy Statement

Surveillance Consisting of Monitoring

(9) The University carries out Surveillance in the form of Monitoring to ensure:

a. the health, safety and welfare of University Employees, students and visitors, for example, by installing fixed cameras throughout University campuses;
b. the integrity, security and service delivery of its systems and Networks; and
c. compliance with its legal obligations, including reporting obligations.

(10) In the course of carrying out Monitoring, the University collects, creates and stores records and information (including logs, images, backups, and archives) using any one or more of the following methods:

a. Telephone Monitoring - the University Monitors the input and output of telephone (both fixed line and mobile) devices provided by the University for use by Employees. These are continually Monitored and may be accessed and provided to the University for administrative purposes;
b. Camera Monitoring - the University has installed fixed security cameras throughout all campuses, both inside and outside of buildings and other facilities. These cameras (including any casings) are not covered or hidden, and Monitor activities on an ongoing and continuous basis;
c. Computer Monitoring - the University conducts ongoing Monitoring of the following:
    i. University email accounts, and emails sent or received using a University email account or a University server;
    ii. internet usage, including browsing history, content downloads and uploads, video and audio file access, and any data input using the IT Resources; and
    iii. access (including logons) to, and all activity on, the IT Resources including computer hard drives and servers, and any files stored on IT Resources;
d. Tracking Monitoring - the University does not Monitor or track the location or movement of individual Employees. However, it does provide and make available for use by Employees equipment and devices that have functionality to monitor and record their geographical location or movement, for example:
    i. mobile telephones, hand-held radios, laptops, tablets and similar devices;
    ii. access cards into University buildings;
    iii. University-owned vehicles with global positioning systems installed;
    iv. fuel cards issued for University-owned vehicles; and
    v. wired and wireless data point connections installed in University buildings.

(11) In carrying out Monitoring, the University records and stores information and creates records (including reports) in relation to the following that are Surveillance Information and Surveillance Records for the purposes of the Act:

a. movements within a Workplace;
b. access to secure University facilities (buildings and locations within buildings);
c. connection of devices (whether or not owned by the University) to IT Resources and the Network. This includes 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 downloading history on IT Resources; and
e. any information or data created or managed on, downloaded to and stored on IT Resources, servers and other devices that the University supplies or otherwise makes available for use, including University email.

Surveillance and Surveillance Information and Records

(12) The University may from time to time:

a. conduct Surveillance, including Surveillance of individual Employees; or
b. access, use or disclose information or records obtained in the course of Monitoring for Surveillance in relation to individual Employees.

(13) The University may use or disclose Surveillance Information or Surveillance Records for purposes authorised under the Act and in accordance with the procedures set out in Section 4 of this Policy. These specifically include:

a. for legitimate purposes related to the employment of Employees;

b. for the legitimate business activities or functions of the University, including 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 as its Employee;
c. for use or disclosure in any legal proceedings (including an inquiry by the Independent Commission Against Corruption or the NSW Ombudsman) to which the University is a party or is directly involved;
d. disclosure to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
e. where otherwise required or authorised by law to do so (for example, if the University is required to comply with a search warrant or subpoena);
f. where the University considers this is reasonably necessary to avert a serious and imminent threat of:
    i. serious violence to a person;
    ii. damage to property (including disruption to the University's business, systems or operations).

(14) Part 4 of the Act prohibits covert surveillance (which is Surveillance other than that requiring notification in accordance with Part B below) by an employer without a covert surveillance authority issued under that Act.

Prohibited Surveillance

(15) The University will not carry out and does not condone any of the following which are prohibited under the Act:

a. Surveillance of Employees in a change room, toilet facility or shower or other bathing facility in the Workplace;
b. Surveillance of Employees using work Surveillance devices when Employees are not at work, except as permitted under the Act and this Policy; and
c. blocking emails or internet access of an employee except as permitted under the Act and University policies, including Part C of this Policy.

Section 4 - Surveillance Procedures

Part A - Authorisation

(16) Employees are prohibited from conducting any form of Workplace Surveillance or from accessing Surveillance Records or Surveillance Information, except the following Employees who are only authorised for the purposes of performing their designated duties as Employees:

a. Employees (including those within Cyber Security Assurance and Operations and Information Technology and Digital Services) whose normal duties include routine back up 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 IT Resources and Networks;
b. Employees (including those in Campus Safety and Security) whose normal duties include review of camera footage and of building access (including use of building access devices); or
c. Employees who are specifically authorised under this Part A to conduct Surveillance or to access Surveillance Information or Surveillance Records.

(17) Requests to authorise Surveillance that go beyond Monitoring, or to authorise access to Surveillance Information or Surveillance Records by persons other than those listed in clause (16), may only be made by one or more of the following persons and only for a purpose specified in clause (13):

a. the Vice-Chancellor and President;
b. the Senior Deputy Vice-Chancellor;

c. a Deputy Vice-Chancellor and Vice-President;
d. a Vice-President;
e. a Dean;
f. the General Counsel;
g. the University Secretary; or
h. the Chief Audit and Assurance Officer.

(18) Only the Vice-Chancellor and President can approve a request on advice from the General Counsel.

(19) For the avoidance of doubt, Surveillance requests made under clause (17) will only be approved if the Vice-Chancellor and President is reasonably satisfied that:

a. the request is for a purpose specified in clause (13);
b. if the request is for a purpose specified in clause 13(b):
    i. there is no less intrusive alternative, reasonably available, in the circumstances, including, but not limited to, any need for urgency;
    ii. the proposed method and length of Surveillance or access to information and records is reasonable and appropriate in the circumstances; and
    iii. reasonable precautions will be taken to ensure the integrity and security of data, including compliance with the University's Privacy Policy and Privacy Management Plan.

Part B - Notice Requirements

(20) This Policy is formal notice to Employees that the University does the following in accordance with this Policy:

a. it conducts Surveillance in the form of Monitoring in the Workplace;
b. where authorised under the Act or this Policy, it conducts Workplace Surveillance other than Monitoring; and
c. it creates, accesses, uses and discloses information or records in relation to Surveillance, including as part of Monitoring.

(21) The University also provides notice to Employees about Surveillance (including Monitoring) in other formats as follows:

a. in the case of Monitoring by cameras, by means of physical signage at the entrances to or within campus grounds;
b. by obtaining a signed acknowledgement when an employee commences employment;
c. by means of regular (usually every six months) reminder notifications to all Employees by the Senior Deputy Vice-Chancellor or Vice-President, Strategy and Governance;
d. by means of an online notice referring to this and other relevant policies when an employee activates their University account for the first time;
e. for new methods of Monitoring, specific written notice to all Employees (which may be given by email) at least 14 days before that routine Monitoring commences.

(22) For Surveillance approved under Part A, the University must send a written notice to an individual employee (which may be given by email) before that Surveillance commences.

(23) A notice under clause (21) e. or (22) must be given or authorised by either the Chief Information and Digital Officer or the University Secretary, and must specify:

a. the type of Surveillance or new form of Monitoring to be carried out;
b. how it will be carried out;
c. when it will start;
d. whether it will be continuous or intermittent; and
e. whether it will be for a specified limited period or ongoing.

(24) Written notice to an employee under clause (22) will not be provided:

a. where there is a risk of disclosure of the identity, or exposure to reprisals, of a person who has made a public interest disclosure under the University's policy relating to public interest disclosures;
b. where Surveillance information or records are aggregated in a format that does not identify specific individuals, including Employees, for example, for operational support reasons.

Part C - Blocking of Email or Internet Use

(25) The Act prohibits the University from blocking an employee from accessing the internet or sending or receiving emails unless:

a. the University acts in accordance with its policies relating to email or internet access that have been notified to the employee in advance in such a way that it is reasonable to assume the employee is aware of and understands the relevant policy; and
b. if the University intends to prevent delivery of an email, the University gives the employee notice (which can be by email) that delivery of the email will be blocked.

(26) The University is not required to give notice under clause (25)b if:

a. the University regards the content of the website or email, including any attachment, as menacing, harassing or offensive, for example, pornographic, gambling or terrorist websites;
b. the email is or contains a commercial electronic message, as defined in the Spam Act 2003 (Cth);
c. the content or attachments of the email would or might result in unauthorised interference with, damage to or operations of an IT Resource (including any program run or data stored on any IT Resource);
d. the sender of the email has been identified as having previously sent malicious content to the organisation;
e. the University is not aware (and cannot reasonably be expected to be aware) of whether an employee has sent that email or of the identity of the employee who has sent that email.

Section 5 - Guidelines

(27) Nil.

Status and Details

Status	Current
Effective Date	16th August 2024
Review Date	3rd September 2025
Approval Authority	Director, Governance Services
Approval Date	16th August 2024
Expiry Date	Not Applicable
Unit Head	Gordon Babe General Counsel 9894
Author	Nicole Bannerman General Counsel 96859895
Enquiries Contact	Gordon Babe General Counsel 9894