

# Workplace Surveillance Policy

## Section 1 - Purpose and Context

(1) The purpose of this policy is to ensure that the University complies with the requirements of the [Workplace Surveillance Act 2005](#). The Policy does not provide for, or signal any changes, to the practices of the University. However, the Act requires that employees be formally notified of any actions by the University that would fall within the definitions of surveillance.

(2) The Act deals with surveillance of employees by means of cameras, computers or tracking devices and requires that employees are notified as to the nature of that surveillance. The notice provided to staff must indicate:

- a. the kind of surveillance to be carried out (camera, computer or tracking)
- b. how the surveillance will be carried out
- c. when the surveillance will start
- d. whether the surveillance will be continuous or intermittent
- e. whether the surveillance will be for a specified limited period or ongoing

(3) Any surveillance type activity that is undertaken by the University must be in accordance with the Act and specifically the notice provided to employees. Any surveillance outside the parameters of the notice is considered to be covert surveillance and must be authorised by a Magistrate.

## Section 2 - Definitions

(4) Under the [Workplace Surveillance Act 2005](#), surveillance of an employee means surveillance of an employee by any of the following means:

- a. 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;
- b. 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);
- c. 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).

## Section 3 - Policy Statement

(5) The University is committed to meeting its statutory obligations under the Workplace Surveillance Act 2005.

(6) Section 4 - Procedures of this policy details instances of activity by the University that are covered by the surveillance provisions, being: camera surveillance; computer surveillance; and tracking surveillance.

(7) The University will also comply with the legal requirements of the Act where surveillance is prohibited. These are

contained in Part 3 of the Act (sections 15 to 18) and cover:

- a. a prohibition on surveillance in any change room, toilet facility, shower or other bathing facility at the workplace;
- b. a prohibition on surveillance when the employee is not at work except in cases of computer surveillance where the employee is using equipment and/or resources supplied by the University. If staff connect to the University via a private computer, such surveillance shall be restricted to University equipment only;
- c. a prohibition on blocking the delivery of emails unless notice (prevented delivery notice) has been given to the employee or where the incoming communication is perceived to be spam or a threat to the security of the University's systems or contains potentially menacing, harassing or offensive material; and
- d. a prohibition on preventing delivery of an email or access to a website merely because it has been sent by or on behalf of an industrial organisation of employees or contains information about industrial matters.

## **Section 4 - Procedures**

(8) Individual staff are prohibited from undertaking surveillance in their workplace. Where it is necessary to undertake new or additional workplace surveillance it will be in accordance with this policy and approved by both the Chief Information Officer and the Director, Campus Safety and Security.

### **Part A - Notification**

(9) The University will provide written notification to staff of surveillance activities that occur at UWS. The University will also periodically remind staff of the surveillance activities and will refer staff to this policy.

(10) The Office of People and Culture will give written notification of surveillance activities at UWS to all new staff before they commence. Such notification will also refer to this policy.

### **Part B - Camera Surveillance**

#### **Security Cameras**

(11) The University operates security cameras on all of its campuses both within and without buildings. This is for the purpose of ensuring the safety and security of staff, students, visitors and the University's premises and facilities. Camera footage may be accessed and used as evidence where an act (e.g. assault of a person, damage to facilities) has occurred that warrants investigation by the University. Such records may also be required by law to be provided to other parties such as a court or to the police.

(12) Notices that the University's campuses are monitored by cameras are located at each of the entrances to the University's campuses. Security cameras are located in and around facilities requiring security monitoring for the safety or security of individuals or property and are not disguised or secreted.

(13) Security cameras are in place as at the date of approval and promulgation of this policy. Camera security monitoring is continuous and ongoing.

#### **Mobile Telephone Cameras**

(14) Cameras in mobile telephones supplied by the University are not to be used to record images of any persons without their knowledge or consent.

## Part C - Computer Surveillance

### General Use of UWS Information Technology Systems and Facilities

(15) Use of the University's computers and associated systems is governed by the [IT Acceptable Use of Resources Policy](#), which prescribes the conditions under which employee access is provided to the University's information technology facilities, services and systems. The IT Acceptable Use of Resources Policy also covers student users.

(16) In accordance with that policy, the Chief Information Officer, authorised staff of Information Technology Services, or other authorised personnel may access University computers, computer logs and other system records, databases and backups to ensure the security, confidentiality, availability and integrity of University IT systems.

(17) From time to time the University may investigate alleged breaches of the law or University policies by staff using its IT systems and facilities and this can involve accessing the staff member's computer and electronic records. For staff, such investigations may involve misconduct or serious misconduct and are managed in accordance with the provisions of the relevant employment agreement.

(18) The University monitors staff use of University computers and IT systems in the following areas:

- a. University workstations, servers, email and network services, printers, network connected devices, and connections to the internet.
- b. The University retains logs, backups and archives of computing activities, which may be audited. Such records are the property of the University, are subject to State and Federal laws and may be used as evidence.
- c. Monitoring may include, but is not limited to; storage volumes, download volumes, breaches of intellectual property laws, suspected malicious code or viruses.

(19) Computer surveillance is intermittent but ongoing and is in place as at the date of approval and promulgation of this policy.

### Email and Internet

(20) Email of staff members is not routinely read or monitored. However, emails are records of the University and should be managed accordingly and will be accessible in that context. An email may also be the subject of a right to information request (under [GIPA](#)) or an application under privacy legislation.

(21) The University may access and monitor staff use of the University email and internet systems in the following ways:

- a. The University monitors email server performance and retains logs, backups and archives of emails sent and received through the UWS server. Even where the user has deleted an email, the University may still retain archived and/or backup copies of the email. Only staff authorised by the Chief Information Officer may examine such records.
- b. The University retains logs, backups and archives of all internet access and network usage. These records may be audited, are subject to State and Federal laws and may be used as evidence. While individual usage is not routinely monitored, unusual or high volume activities may warrant more detailed examination.
- c. For the purposes of producing the email in response to a legal requirement or other lawful investigation.
- d. For the purpose of determining, as part of an investigation by the University, whether there has been unacceptable use of email.
- e. For the purpose of determining whether there has been a breach of the University's policies in the use by the staff member of the University's resources to access the internet.
- f. For the purpose of investigating allegations of misconduct or to provide materials to external investigative

authorities lawfully investigating possible criminal conduct.

(22) Specific provisions related to access to email messages held on the University's servers are contained in the [Email Policy](#).

(23) Email and Internet surveillance is intermittent but ongoing and is in place as at the date of approval and promulgation of this policy.

## **Part D - Tracking Surveillance**

(24) The University currently does not operate any tracking devices of the kind provided for in the legislation. Should the University in the future utilise any tracking devices (such as Global Positioning System tracking devices) for its equipment staff will receive formal notification and this policy will be updated. The purpose of such tracking devices would be to maintain safety and security and not to monitor the location of staff.

## **Section 5 - Guidelines**

(25) Nil.

## Status and Details

<b>Status</b>	Historic
<b>Effective Date</b>	22nd October 2012
<b>Review Date</b>	22nd June 2015
<b>Approval Authority</b>	Vice-Chancellor and President
<b>Approval Date</b>	19th October 2012
<b>Expiry Date</b>	9th October 2014
<b>Unit Head</b>	Philip Maloney General Counsel p.maloney@westernsydney.edu.au
<b>Author</b>	Tanya Rubin
<b>Enquiries Contact</b>	Office of General Counsel