WESTERN SYDNEY
UNIVERSITY

NOTICE TO ALL UNIVERSITY STAFF
WORKPLACE SURVEILLANCE

This is a notice for the purposes of the *Workplace Surveillance Act* 2005 (NSW) and clause 21 (c) of the University's *Workplace Surveillance Policy*, which require that University employees (being University employees and employees of the controlled entities of the University) be notified of surveillance arrangements in their workplaces. The Act and the Policy apply to all University employees and to external providers engaged to provide surveillance services across the University.

Policy

The University has in place a *Workplace Surveillance Policy*, a copy of which can be accessed at https://policies.westernsydney.edu.au/view.current.php?id=00171. Workplace surveillance is only permitted for the purposes and in the manner specified in the Act and in that Policy. It is very important that University employees familiarise themselves with the Policy and with other, related policies, including those relating to acceptable use of IT resources.

The Policy regulates two types of workplace surveillance: surveillance in the form of routine monitoring (described below) and active surveillance for investigation and other purposes.

Purpose of conducting routine monitoring surveillance

The University carries out routine monitoring surveillance to ensure:

- the health, safety and welfare of University employees, students and visitors;
- the integrity, security and service delivery of its systems and networks;
- compliance with the University's legal obligations, including reporting obligations.

How routine monitoring surveillance is carried out

Routine monitoring surveillance is only carried out by University staff (such as ITDS staff or Campus Safety and Security staff) whose normal duties include routine backup or restoration of data, conduct of audits, review of web filtering, email filtering, document retrieval and other activities relating to the University's systems. Routine monitoring does not involve actively investigating or keeping track of individuals or their activities or movements and occurs in one or more of the following ways:

- ***Telephone monitoring*** of input and output of both fixed line and mobile devices supplied by the University and provided for the use of University employees. These devices are continually monitored and may be accessed and provided for administrative purposes;
- ***Camera monitoring*** by means of fixed security cameras which are installed throughout University campuses (both inside and outside buildings) and other facilities. These cameras (including casings) are not covered or hidden. They visually monitor movement and activities on an ongoing and continuous basis;
- ***Computer monitoring***, which is on an ongoing basis of:
    a) University email accounts and emails sent or received using a University email account or a University server;
    b) internet usage, including browsing history, content downloads and uploads, video and

audio file access, and any data input using University IT resources; and

c) access (including logons) to and all activity on University IT resources including computer hard drives and servers and any files stored on University IT resources.

- The University does not monitor or track the location or movement (***tracking monitoring***) of individual employees as part of any routine monitoring. However, it does provide and make available for use by employees equipment and devices (such as mobile phones, building access cards, University vehicles with GPS installed, and building data points) that have the functionality to monitor and record geographical location or movement.

Workplace surveillance other than routine monitoring

The University may conduct workplace surveillance, other than routine monitoring surveillance, provided it meets the requirements of the Act and the Policy. These forms of surveillance may include telephone monitoring, camera monitoring, computer monitoring or tracking monitoring (as described above).

The University does not carry out or condone any of the following:

- surveillance of employees in a change room, toilet facility, shower or other bathing facility in the workplace;
- surveillance of employees using surveillance devices when employees are not at work, except as permitted under the Act and the Policy;
- blocking emails or internet access of employees, except as permitted under the Act and relevant University policies.

Surveillance information and records

When the University conducts surveillance (including routine monitoring) it creates and stores surveillance information or records which it may use or disclose for purposes authorized under the Act and the Policy. These specifically include:

- for legitimate purposes related to the employment of University employees;
- for the university's legitimate business activities or functions, including internal inquiries and investigations relating to activities alleged to be unlawful or in breach of University policies or employee duties;
- for use or disclosure in legal proceedings or inquiries to which the University is a party or is directly involved;
- disclosure to a law enforcement agency (including the policy) as part of an investigation, detection or prosecution of an offence;
- if required by law to do so (for example, comply with a subpoena, search warrant or other court order);
- where the University considers this reasonably necessary to avert a serious and imminent threat of serious violence to a person or damage to property (including disruption to the University's business, systems or operations).