Surveillance Policy

1. Purpose

1.1 The Surveillance Policy (the policy) provides:

- notice to UTS staff, students, affiliates and visitors of the circumstances, nature and types of surveillance at UTS (a requirement for staff and affiliates under the Workplace Surveillance Act 2005 (NSW))
- advice on the systems and processes used by UTS to ensure the security of UTS assets against theft, fraud, malicious or accidental damage and other security breaches.

2. Scope

2.1 This policy applies to all UTS staff, students, affiliates and visitors ('campus users') with access to UTS properties, equipment, IT resources and/or networks.

3. Principles

3.1 UTS is committed to ensuring the security of all campus users, assets and property. This includes the use of surveillance systems (including CCTV) to both discourage and detect any unlawful behaviour in and around university property.

3.2 Surveillance systems are also used to ensure operational efficiency (including traffic management, identification of breakages and malfunctions) and, where necessary, assisting access control and identifying persons of interest (at the request of law enforcement agencies).

3.3 UTS seeks to provide transparency in the circumstances, nature and types of surveillance conducted by the university and comply with the requirements of the Workplace Surveillance Act.

4. Policy statements

4.1 This policy constitutes the provision of notice to campus users of UTS surveillance activities as required under the Workplace Surveillance Act.

Surveillance at UTS

4.2 UTS uses live and recorded monitoring surveillance systems to ensure the health, safety, welfare and security of campus users.

4.3 UTS does not use monitoring surveillance inside private or other specifically designated areas including bathrooms, parents' rooms, changing rooms and prayer rooms.

4.4 All UTS cameras are visible and/or sign-posted. UTS does not use hidden or covert cameras, or dummy cameras.

4.5 UTS does permit the use of hidden and covert cameras by police or other law enforcement authorities on campus and/or by court order.

4.6 All monitoring surveillance systems, applications and monitoring specifications used on UTS campus or property must be approved in line with the UTS Security Standards (Electronic Security) approved by the Manager, Security Services. These standards are available from Security Services upon request.

4.7 The Manager, Security Services will develop and approve appropriate standard operating procedures. These procedures will apply to all monitoring surveillance systems to ensure that:

- all equipment is effectively and appropriately managed, and
- all recorded information is appropriately used, maintained and disclosed in line with the university's Privacy Policy, Data Governance Policy and Records Management Policy.

4.8 All installed monitoring surveillance systems at UTS must be:

- located in a structurally sound, electronically accessed and monitored area that is secure from a risk perspective, with access limited only to authorised users
- integrated into the university's wider electronic security network to enable effective monitoring by Security Services.

Tracking technology at UTS

4.9 UTS does not actively monitor or track the location or movement of individual staff or students. On request, or if required, this information may be passed to law enforcement authorities.

4.10 UTS owns, uses, distributes and provides equipment that has (or may have) the function and capability to record the geographical location of campus users including, but not limited to:

- access passes (including staff and student cards or visitor cards)
- IT equipment (including mobile phones, computers, tablets, smart devices etc)
- radio equipment (including two-way radio equipment)
- UTS fleet vehicles (see definition in Parking at UTS Vice-Chancellor's Directive)
- duress buttons
- security audit systems (including a wanding tool for on-person metal detection)
- electronic key access pads (for cabinets, labs, locker rooms and other secure areas).

Disclosure of surveillance records

4.11 UTS may use or disclose surveillance records where required or permitted under legislation, including:

- at the request of law enforcement or an independent body (eg the Independent Commission Against Corruption, the New South Wales Ombudsman)
- to process requests made under the Government Information (Public Access) Act 2009 (NSW) or NSW privacy legislation
- to assist police, security services or other law enforcement agencies with investigations or otherwise required or authorised to do so by law (eg comply with a warrant or subpoena or to detect and prosecute an offender)
- to assist with internal investigations or legal matters
- to manage any serious matters relating to all campus users
- for training, continuous improvement purposes or compliance for emergency processes (eg emergency evacuations), and/or
- for trend analysis or compliance purposes.

5. Policy ownership and support

5.1 **Policy owner:** The **Deputy Vice-Chancellor (Resources)** is responsible for policy enforcement and compliance, ensuring that its principles and statements are observed. The Deputy Vice-Chancellor (Resources) is also responsible for the approval of any associated university level procedures.

5.2 **Policy contact**: The **Manager, Security Services** is responsible for UTS security systems, the day-to-day implementation of this policy and acts as a primary point of contact for advice on fulfilling its provisions under the Workplace Surveillance Act 2005. The Manager, Security Services (in consultation with the Director, Facilities Management Operations) is also responsible for the approval of security related guidelines and standard operating procedures.

5.3 **Others**

UTS Security Services are the staff (including contractors) responsible for the delivery of security related services at UTS.

6. Definitions

The following definitions apply for this policy and all associated procedures. These are in addition to the definitions outlined in Schedule 1, Student Rules.

Access passes means staff cards, student cards and access cards issued by UTS Security Services.

Affiliates are defined in the Code of Conduct.

Authorised user means a person authorised by the Manager, Security Services (or their delegate(s)) who have successfully completed the approved security training, including a familiarity with this policy and relevant legislation.

Campus users means all those within the scope of this policy as outlined in section 2.

Closed circuit television (CCTV) system means any combination of cameras, lenses, digital or other video recorders and/or accessories and backend systems installed for the purpose of monitoring and/or recording visual activity.

Corporate data is defined in the Data Governance Policy.

Dummy cameras means false or imitation cameras or recording devices.

Monitoring surveillance systems means a device or group of devices and applications used to undertake live and recorded surveillance including but not limited to:

- fixed cameras
- pan, tilt and zoom (PTZ) CCTV cameras
- mobile CCTV cameras, and
- body worn CCTV cameras.

Staff is defined in the Code of Conduct.

Student, for the purposes of this policy, is defined in the Student Rights and Responsibilities Policy.

Surveillance means a form of supervision and monitoring by use of a monitoring surveillance system, tracking surveillance or UTS Security Services staff.

Approval information

Policy contact	Manager, Security Services
Approval authority	Vice-Chancellor
Review date	2022
File number	UR19/2765
Superseded documents	None

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	05/09/2019	12/12/2019	New policy.

Web version

Surveillance Policy

References

Legislation

Government Information (Public Access) Act 2009 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW)

Workplace Surveillance Act 2005 (NSW)

UTS documents

Code of Conduct

Data Governance Policy

Privacy Policy

Records Management Policy

Student Rights and Responsibilities Policy

UTS Security Standards (Electronic Security) (request from Security Services)

External bodies

Independent Commission Against Corruption

New South Wales Ombudsman

Contacts

New South Wales Police

Security Services general email: security.general@uts.edu.au