Surveillance Policy

NIDA

1. POLICY STATUS AND DETAILS

Policy Number	SP01
Approving Authority	NIDA Board
Date Implemented	2024-08-28
Current Version	1.0
Date of Review	2027-08-28
Contact Officer	Chief Operating Officer
Related Policies, Procedures and Documents	NIDA Code of Conduct and Student Charter Acceptable Use of information Technology Resources Policy Critical Incident Policy Misconduct Policies Privacy Policy WHS Policy Record Keeping Policy

1. PURPOSE

1.1 The Surveillance Policy:

a) outlines the cirucmstances, nature and kinds of surveillance at NIDA

b) is notice of surveillance under the Workplace Surveillance Act 2005 (NSW), and

c) describes the systems and processes used to ensure the security of assets and other security breaches

2. SCOPE

This policy applies to all campus users with access to NIDA property, equipment, information technology resources and/or networks.

3. PRINCIPLES

3.1 NIDA seeks to provide transparency in relation to the nature and types of surveillance employed and complies with the requirments of notification under the Workplace Surveillance Act 2005 (NSW). NIDA gives notice of surveillance to all campus users in line with section 10 of the

workplace Surveillance Act

3.2 NIDA is committed to ensuring the safety and secruity of all campus users, assets and facilities

3.3 Surveillance is also used to ensure operational efficiency and identification of breakages, malfunction of equipment and damage to facilities

3.4 NIDA is committed to balancing all users right to privacy with the legitimate protection and proper usage of NIDA IT resources. NIDA will take reasonable precautions to protect the privacy of users, however, the use of NIDA IT Resources is not considered a private action or conduct.

3.5 Where necessary, NIDA surveilance systems may be used to collect information or identify persons of interest in the event of an incident or at the request of a government agency inlcuing but not limited to law enforcement agencies.

4. POLICY

4.1 Surveillance

4.1.1 NIDA uses live and recorded monitoring surveillance systems to ensure the health, safety, wellbeing and security of NIDA campus users. This includes corridors, all theatres, public spaces and in some workshops where misuse of machinery can cause serious injuries.

4.1.2 NIDA does not have monitoring surveillance systems in bathrooms, dressing rooms or in regualar rehearsal rooms and studios.

4.1.3 Cameras will be visible and NIDA signposts all cameras. Dummy cameras or hidden cameras are not used unless required to do so by law enforcement or by court order.

4.1.4 All NIDA Digital Information stored, processed, or transmitted using any NIDA Information Resource:

a. may be recorded and monitored on an ongoing and continuous basis,
b. may be subject to the Government Information (Public Access) Act 2009 (NSW).
c. may be subject to the Privacy and Personal Information Protection Act 1998 (NSW).
d. may be subject to the Health Records and Information Privacy Act 2002 (NSW).
e. may be subject to the State Records Act 1998 (NSW).
f. will remain in the custody and control of NIDA.

4.1.5 NIDA Digital Information may be retained for as long as required in accordance with relevant statutes, regulations, or for archival purposes and business needs in line with NIDA's Record Keeping Policy.

4.2 Surveillance Systems

4.2.1 The Chief Operating Officer must also develop and approve appropriate standard operating procedures. These procedures must apply to all monitoring surveillance systems to ensure that;

a. all equipment is effectively and appropriately managed, and
b. all recorded information is used, maintained and disclosed in line with the NIDA Privacy Policy, the Record Keeping Policy,

4.2.2 All monitoring surveillance systems at NIDA must be:

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

4.2.3 NIDA may conduct surveillance by:

a. accessing, monitoring, logging and recording any communication or information developed, used, received, stored or transmitted by a staff member or student using the NIDA's IT Systems (either on NIDA campus or at any other place and including a private use of NIDA's IT Systems);
b. installing filtering systems in NIDA'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.

6.3 Tracking technology at NIDA

6.3.1 NIDA 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:

a. access cards (including staff and student cards or visitor cards)
b. IT equipment (including mobile phones, computers, tablets and smart devices)
c. Radio equipment (including two-way radio equipment)
d. electronic key access pads (for cabinets, locker rooms and other secure areas)

6.3.2 NIDA Systems may passively track individuals without active monitoring with exceptions of the NIDA Theatres. These systems are employed for security and surveillance, record movements and activities in their field of view or scope of application. While not always actively watched or reviewed, the footage can be reviewed retrospectively to identify patterns, behaviours, or specific events.

6.4 Disclosure of Surveillance Records

NIDA may use or disclose surveillance records where it has a reasonable basis, unless prohibited by law and when required or permitted under law, including:

a. at the request of a law enforcement agency or an independent body (for example, the Independent Commission Against Corruption and the New South Wales Ombudsman)
b. to process requests made under the Government Information (Public Access) Act 2009 (NSW) or NSW privacy legislation

c. to assist NIDA Management, police or other law enforcement agency with investigations or otherwise required or authorised to do so by law (for example, to comply with a warrant or subpoena or to detect and prosecute an offender)
d. to assist with internal investigations or legal matters
e. to manage any serious security matter relating to a NIDA campus user
f. where it is reasonably believed to be necessary to avoid an imminent threat of serious violence

6.5 Misconduct

6.5.1 Allegations of interference with, including blocking and moving, or damage to NIDA surveillance cameras by a NIDA student is misconduct and will be managed in accordance with NIDA's Misconduct Policy.

6.6 Complaints

6.6.1 Complaints by students should be made in writing using the Non-Academic Complaints and Appeals form https://nida.qualtrics.com/jfe/form/SV_6rJSRRSxFSbBiL4

5. DEFINITIONS

Term	Definition
Campus	Any building, vehicle or asset under NIDA management or the immediate vicinity of the building
Campus user	Any staff member, student, visitor, contractor or affiliate who is on campus or engaging with NIDA facilities
Surveillance camera	Cameras used for monitoring spaces, entrances or machinery use that can be continuously recording or only recording when triggered by movement.
Monitoring surveillance system	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.

Surveillance	Surveillance is defined under section 3 of the Workplace Surveillance Act 2005 (NSW). In summary, it refers to monitoring and recording through the use of security cameras, computers or other devices that may have the ability to track location or movement information.

6. CHANGE HISTORY

Date	Change Description	Reason for	Author	TRIM/CM
February 2024	New Policy	Roll out of cameras in corridors and workshops	Chief Operating Officer	

7. CONSULTATION/BENCHMARKING

Benchmarked against policies and practice from several higher education providers and other sources.

Relevant policy documents from the following are gratefully acknowledged:

- Sydney University
- University of New South Wales (UNSW)
- University of Technology Sydney (UTS)
- Western Sydney University
- Macquaire University
- Melbourne University Student Union

Consultation: TBA

Legislation and Regulatory Frameworks	Workplace Surveillance Act 2005 (NSW) Privacy & Personal Information Protection Act 1998 (NSW)