AFTRS
Australian Film Television and Radio School

# Surveillance of Facility, Device and Systems Policy

## Table of Contents



## 1. Purpose

1.1. This policy outlines the circumstances under which the Australian Film, Television and Radio School (**AFTRS**) conducts workplace and student surveillance. It ensures compliance with the *Workplace Surveillance Act 2005* (NSW) and provides clear information to employees, students and AFTRS facility users on how surveillance is conducted, used, and managed at AFTRS.

1.2. AFTRS is committed to maintaining a safe and secure working and learning environment while respecting the rights and privacy of all individuals within its premises and digital platforms.

1.3. AFTRS will conduct ongoing and intermittent computer surveillance of all users and devices - including personally owned devices that access AFTRS IT facilities and services - for the following purposes:

- To comply with legislative requirements;
- To protect its assets, property, and finances from unlawful activities or breaches of AFTRS policy or rules;
- To support its business and operational requirements;
- To meet stakeholder and public expectations; and
- To protect its reputation.

1.4. AFTRS is committed to complying with its obligations under the Workplace Surveillance Act 2005 (NSW). This policy serves as formal notification to users of surveillance activities that fall under the definition of computer surveillance.

## 2. Scope

2.1. This policy applies to:

- All AFTRS employees, including full-time, part-time, and casual staff.
- Students, Award Course or otherwise; including full-time, part-time, on-campus, and remote learners.
- Contractors, consultants, and third-party personnel who have access to AFTRS premises, equipment, or IT systems.
- AFTRS facility visitors and users
- All AFTRS-controlled environments, including physical campuses, digital platforms, and remote work and learning systems.

2.2. This policy does not apply to surveillance conducted by external law enforcement agencies or third-party service providers outside of AFTRS' control.

## 3. Definitions

| | |
|---|---|
| ***Surveillance*** | The monitoring of workplace and student activities through cameras, IT systems, or tracking mechanisms. |
| ***Employee*** | All AFTRS staff, including full-time, part-time, casual. |
| ***Student*** | All individuals enrolled in AFTRS courses including full-time, part-time, and online learners. |
| ***IT Resources*** | AFTRS-managed hardware, software, and networks. |
| ***Monitoring*** | Routine data collection for security, compliance, and academic integrity purposes. |
| ***Workplace and Study Environment*** | Any AFTRS-controlled space where employees and students engage in work or learning activities. |

## 4. Principles

4.1. AFTRS seeks to provide transparency in relation to the nature and types of surveillance employed and complies with the requirements of notification under the Workplace Surveillance Act 2005 (NSW).

4.2. AFTRS is committed to ensuring the safety and security of all campus users, assets and facilities.

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

4.4. AFTRS is committed to balancing users' right to privacy with legitimate protection and proper uses of AFTRS IT resources. AFTRS will take reasonable precautions to protect the privacy of users, however the use of AFTRS IT resources is not considered a private action or conduct.

4.5. Where necessary, AFTRS surveillance 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, including but not limited to law enforcement agencies.

# 5. Policy Statement

## Types of Surveillance

5.1. AFTRS conducts surveillance in accordance with NSW workplace and educational institution laws. Surveillance may be carried out through the following means:

### Camera Surveillance

5.1.1. Surveillance cameras are installed in strategic locations on AFTRS campuses and facilities for security and safety purposes.

5.1.2. Surveillance cameras are clearly visible and not placed in classrooms or private areas such as restrooms or changing rooms.

### Computer and Digital Surveillance

5.1.3. AFTRS monitors IT systems to ensure security, compliance, and appropriate use of resources by staff, students, and contractors, consultants, and third-party personnel who have access to AFTRS premises, equipment, or IT systems.

5.1.4. Computer surveillance may include, but is not limited to:

- Accessing AFTRS email accounts and messages;
- Accessing files stored on AFTRS systems;
- Accessing AFTRS systems and their activity logs (Example Moodle);
- Accessing work devices and their activity logs;
- Recording and reviewing internet usage;
- Accessing telephone usage logs; and
- Accessing personal devices used for AFTRS business.

### Tracking Surveillance

5.1.5. AFTRS **does not** routinely track individuals; however, may record access to facilities via:

- Building swipe card logs (e.g., entry to classrooms, labs, and secured areas).
- GPS tracking on AFTRS-owned equipment (e.g., loaned cameras, laptops, and vehicles where applicable).

## Use of Surveillance Information

5.2. Surveillance information may be used for:

- Ensuring campus security and preventing unauthorised access.
- Investigating misconduct or policy breaches by employees or students.
- Compliance with legal requirements, including responding to law enforcement requests.
- Supporting academic integrity and IT security measures.
- Access to surveillance data is restricted to authorised personnel and managed in accordance with privacy laws and AFTRS policies.

## Notification and Consent

5.3. Employees and students are made aware of surveillance through:

- Signage at locations where camera surveillance occurs.
- Employment agreements and student enrolment terms, which reference IT and digital surveillance policies.

## Prohibited Surveillance

5.4. AFTRS does not conduct:

- Concealed or secret surveillance, unless explicitly authorised by law.
- Employment monitoring of private areas, such as restrooms, changing rooms, or private study spaces.

- Surveillance of employees or students outside AFTRS activities, unless using AFTRS-owned devices for academic or work-related purposes.
- Internet and email access may be monitored and restricted if deemed a security risk, such as in cases of phishing, malware, or inappropriate content.

# 6. Surveillance Procedures – Authorisation

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

- Employees (including those with Cyber Security, Information Technology and Business Application Systems) 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 AFTRS' networks and IT systems.
- Employees (including those in Facilities) and on campus Security personnel whose normal duties include review of camera footage and of building access.
- Employees who are specifically authorised to conduct Surveillance or to access Surveillance Information or Surveillance Records Responsibilities.

6.2. Requests to authorise Surveillance that go beyond Monitoring, or to authorise access to Surveillance Information or Surveillance Records by persons other than list in clause 5.1 above), maybe be made by one or more of the following persons and only for a purpose specified in Clause 4.2:

a. the Chief Executive Officer
b. the Director of People and Culture

6.3. For the avoidance of doubt, Surveillance requests made under clause 5.2 will only be approved if the Chief Executive Officer and the Director of People and Culture is reasonably satisfied that:

a. the request is for purposes as those specified in clause 4.2;
b. there is no less intrusive alternative, reasonable available, in the circumstances, including but not limited to, any need for urgency;
c. if the proposed method and length of Surveillance or access to information and records is reasonable and appropriate to the circumstances; and
d. reasonable precautions will be taken will be taken to ensure the integrity and security of data.

# 7. Responsibilities

### Compliance, monitoring and review

7.1. The Director of Production Technology & Infrastructure is responsible for:

- Ensuring surveillance aligns with legislation and AFTRS policies.
- Conducting periodic reviews to assess policy effectiveness.
- Addressing any emerging security concerns related to staff and students.
- Reviewing the Surveillance of Facility, Device and Systems Policy will be reviewed every three years from effective date or earlier or later, depending on external factors such as legislative reform.

### Reporting

7.2. No additional reporting is required unless surveillance data is used in an investigation, academic integrity case, or legal process. In these cases the surveillance data used will be stated in investigation report or case file records.

- Employees or students who have concerns about surveillance practices may raise queries with, HR, IT Security or Student Centre.

7.3. Any misuse or unauthorised access to surveillance data must be reported immediately to AFTRS management.

**Records Management**

7.4. All records relevant to administering this policy will be maintained by the Policy and Governance Officer.

7.5. All surveillance records are:

- Stored securely in compliance with AFTRS data policies.
- Accessed only by authorised personnel.
- Retained for the legally required period before secure disposal.

## 8. Related Legislation and Documents

- *Workplace Surveillance Act 2005* (NSW)
- *Privacy Act 1988* (Cth)
- Employee Code of Conduct
- Student Code of Conduct (Student Handbook)
- Privacy Policy
- IT Acceptable Use Policy

## 9. Approval and Review Details

| Approval and Review | Details |
|---|---|
| Approval Authority | CEO |
| Responsible Officer | Director of Production Technology & Infrastructure |
| Contact Officer | Director of Production Technology & Infrastructure |
| Distribution | Intranet and AFTRS website<br>Staff and Public facing |
| Next Review Date | **01 August 2028** |

| Approval and Amendment History | Details |
|---|---|
| Original Approval Authority, date and details | CEO, 18 August 2025 – no amendment as is new document |
| Amendment History and Date | N/A<br><<DD/MM/YYYY —Amendment detail; DD/MM/YYYY—Amendment detail >> *[Include the previous approval authority approval dates and corresponding amendment detail. This section ill will expand over time. In the case of a brand new policy doc, insert N/A]* |
| Notes | N/A |
| Minor Amendment Approval and History | N/A<br><<DD/MM/20YY — Xxxxx>><br>• ***[A minor amendment consists of an administrative edit made to the document or a change that is not material to the document.***<br>• ***The Responsible Officer can approve a minor amendment.***<br>• *Insert the date that the Responsible Officer approved the minor amendment along with the details of the amendment (For example: "01/12/2020 —administrative amendment: update of role titles aligned to restructure", or insert, if not relevant, N/A [If making a minor amendment, do not amend details in the Original Approval Authority section nor amend the version numbe**r, only replace the new minor amendment approval date to the file**]* |