FAYETTEVILLE STATE UNIVERSITY

SURVEILLANCE TECHNOLOGY

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	Information Technology
Applies to:	● Administrators ●Faculty ●Staff ●Students
History:	First Issued – June 13, 2025
Related Policies/	Physical and Environmental Security
Regulations/Statutes	Law Enforcement Agency Recordings [NCGS 132-1.4A]
Contact for Info:	Associate Vice Chancellor for Police and Public Safety (910) 672-1775 Chief Operations Officer| (910) 672-1200

I. PURPOSE

The purpose of this policy (Policy) is to provide a governance structure and guidelines for the use of surveillance technology (Surveillance Technology) at Fayetteville State University (University). This Policy promotes the effective use of University electronic surveillance technology for safety and security purposes while preserving respect for individual privacy and ensures the use of video surveillance technologies in a consistent, ethical, and appropriate manner at the University. Also, this Policy outlines the requirements for recording, handling, viewing, retention, dissemination, and destruction of live and recorded images captured by Surveillance Technology and establishes clear guidelines to ensure proper management and privacy protection throughout the image lifecycle.

II. SCOPE

This policy applies to all Surveillance Technology deployed in public spaces owned, operated and leased by the University.

A. Surveillance Technology

Surveillance Technology is any technology that collects, captures, or records audio, visual, or other forms of information for the purpose of monitoring activity. This includes, but is not limited to, the use of cameras, video recording devices, and other electronic monitoring equipment intended for security and law enforcement purposes

This Policy is not applicable to recorded media related to student education, research activities, artistic or creative performances, or athletics. Such recordings are governed by separate University guidelines that address their specific use cases and regulatory requirements. This Policy is also not applicable to licensed plate recognition systems (LPRs). Questions regarding LPRs should be directed to the Associate Vice Chancellor for

Police and Public Safety (Chief of Police).

B. Public Spaces

Public Spaces include property that is within the campus or immediately adjacent and accessible from the campus. For the purposes of this Policy, Public Spaces shall include, but not be limited to, parking areas, law enforcement vehicles, streets, walkways, thoroughfares, and building interior or exterior areas, excluding any space where an occupant would have a reasonable expectation of privacy.

III. AUTHORIZED USE

Surveillance Technology may be used for legitimate safety, security or law enforcement purposes under the approval of the Department of Police and Public Safety (DPPS) in collaboration with the Division of Legal, Audit, Risk, and Compliance (LARC). Safety, security, and law enforcement purposes include, but are not limited to, deterring criminal activity, conducting criminal investigations, and promoting campus safety and security. DPPS may also use body worn cameras in any spaces that are consistent with DPPS's Standard Operating Procedures on Body Worn Cameras.

Additionally, Surveillance Technology must meet the technology standards approved by the Office of Information Technology Services (ITS).

IV. DEPLOYMENT

Surveillance Technology shall only be deployed in Public Spaces where there is a reasonable expectation of safety or security. Surveillance of private areas such as residence hall rooms, restrooms, and private offices are prohibited unless required by law or authorized by court order.

The location of Surveillance Technology shall be determined by DPPS in coordination with ITS. Signs shall be posted to inform the public of the use of surveillance technology.

V. MONITORING

Under normal operating conditions, Surveillance Technology is not intended to be actively monitored at all times, but may be monitored as needed for legitimate safety and security purposes, that include but are not limited to monitoring the following: areas where an alarm has been triggered; areas identified as high risk due to existing safety or security concerns; restricted access areas; areas where special events are occurring; and areas under specific investigations authorized by DPPS.

The monitoring of individuals or groups of individuals through live feed or recorded images will be based on behaviors that potentially violate law or University policy and such monitoring must be conducted in a manner consistent with applicable laws and policies.

VI. DATA STEWARDSHIP

A. Collection and Retention

Data collected as a result of the use of Surveillance Technology shall be stored securely and shall only be accessible to authorized personnel designated by DPPS leadership.

Data will be retained for no longer than 60 days unless required for ongoing investigations, legal proceedings, or the UNC System Records Retention Schedule. Data will then be destroyed in compliance with the UNC System Records Retention Schedule.

The unauthorized dissemination of surveillance data is strictly prohibited.

B. Access and Use of Data

Only authorized personnel within DDPS may access or use data obtained from Surveillance Technology. Such access shall be in compliance with state and federal law including but not limited to NCGS 132-1.4A which governs law enforcement agency recordings.

Only the Chief of Police may authorize access to date requested by external law enforcement agencies. Non-law enforcement requests for access to data must be approved by LARC and the Chief of Police and must be in compliance with applicable state and federal laws.

Any unauthorized access to Surveillance Technology, including but not limited to, the inadequate protection, inappropriate use, disclosure, or disposal of live or recorded images or data must be reported immediately to LARC.

VII. PRIVACY CONSIDERATIONS

The University is committed to balancing security needs with the right to privacy. Surveillance Technology shall not be used to monitor individuals or groups based on race, gender, ethnicity, or other protected characteristics unless such monitoring is related to a specific criminal investigation.

DPPS shall conduct periodic reviews of Surveillance Technology deployments to ensure compliance with departmental requirements, University policies, and state and federal laws. Upon request by the University's General Counsel, an audit report will be provided by the Chief of Police or his/her designee.

VIII. COMPLIANCE AND ENFORCEMENT

Any person in violation of this policy may be subject to disciplinary action in accordance with university policies and procedures and may be subject to criminal sanctions under NCGS and federal laws.