

Policy 425

Automated License Plate Readers (ALPRs)

425.1

PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

425.2

POLICY

The policy of the New York State University Police at Delhi is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public and employees.

All data and images gathered by the ALPR are for the official use of SUNY Delhi and overseen by the New York State University Police of Delhi.

425.3

ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the New York State University Police at Delhi to utilize data associated with vehicle license plates for official law enforcement purposes, including but not limited to identifying stolen or wanted vehicles, stolen license plates, and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, stolen property recovery, and the investigation of suspicious or suspected criminal activity (such as those listed under 425.4).

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Chief of Police. The Chief of Police will assign a Lieutenant to administer the day-to-day operation of the ALPR equipment and data.

425.4

OPERATIONS

Use of an ALPR is restricted to the purposes outlined in this policy, for Police and SUNY Delhi business. University Police Department members shall not use, or allow others to use, the ALPR equipment, system, or data for any unauthorized purpose.

The ALPR system shall be used for collecting ALPR Hits for investigations related but not limited to:

- Criminal activity;
- Stolen or wanted vehicles;
- Stolen license plates;
- Wanted persons;
- Missing/endangered persons;

- Vehicles with known associated exclusions from SUNY Delhi's campus (including and related protection orders);
- Threats to persons or property;
- Emergent situations related to public safety;
- Suspected criminal activity and other police investigations;
- Traffic flow/volume data (raw vehicle numbers - no license plate data)

425.5

DATA COLLECTION AND RETENTION

The Chief of Police is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. The ALPR vendor is contractually obligated to store the data and ensure proper maintenance and security of data stored in its data towers. The ALPR vendor will purge data at the end of ninety (90) days of storage. However, this will not preclude NYSUP from maintaining any relevant vehicle data from the system related to police investigations after the ninety days pursuant to relevant NYS retention schedules.

The ALPR vendor is not permitted to share or sell ALPR data. The ALPR vendor is prohibited by NYSUP policy and by contract from sharing or providing access to any ALPR data collected to any other entity

425.6

ACCOUNTABILITY AND SAFEGUARDS

All data will be closely safeguarded and protected by both procedural and technological means. The New York State University Police at Delhi will observe the following safeguards regarding access to and use of stored data:

- a. All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access to information by name, date, and time.
- b. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement or SUNY Delhi business purposes only. The following uses of the ALPR system are specifically prohibited:
 1. Invasion of privacy - except when done pursuant to a court order, legally binding subpoena, or legally binding search warrant, it is a violation of this policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view on campus roadways.
 2. Harassment or intimidation - It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.
 3. Use based on a protected characteristic - It is a violation of this policy to use the ALPR system or associated data or hot lists solely because of a person or group's race, gender, age, religion, political affiliation, nationality, ethnicity, sexual orientation, sexual identity, disability, veteran's status, or other classification protected by law.
 4. Personal use - It is a violation of this policy to use the ALPR system or associated data or hot lists for any personal purpose.
 5. First Amendment rights - It is a violation of this policy to use the ALPR system or associated data or hot lists for the purpose or known effect of infringing upon First Amendment rights.

6. This system is implemented for safety, security, and operational purposes and is not designed for employee monitoring. The system will not be used to evaluate employees, to monitor their performance, or for taking attendance.

425.7

RELEASING ALPR DATA to external entities

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- a. The agency makes a request for the ALPR data that includes:
 1. The name of the agency.
 2. The name of the person requesting.
 3. The intended purpose of obtaining the information.
- b. The request is reviewed by the Chief of Police or authorized designee and approved before the request is fulfilled.
- c. The approved request is retained on file.
- d. The sharing of ALPR data is subject to the terms of any existing sharing agreement with the regional Crime Analysis Center.
- e. Subject to State University of New York policies and procedures.

425.8

Training

All authorized personnel must complete training on ALPR systems and data prior to active use and be provided with all applicable College policies and procedures. Training must include:

- a. How to use the ALPR technology;
- b. Knowledge and understanding of the College's ALPR policy and procedures; and
- c. Applicable laws and privacy protections.

425.9

Sanctions

Violations of this policy will be dealt with in accordance with applicable College policies and procedures. Failure to comply with this policy may result in sanctions relating to an individual's employment (up to and including termination of employment in accordance with applicable College policy and collective bargaining agreements); civil liability; or any combination of these.

DEFINITIONS

Automated License Plate Reader (ALPR)

A device that uses cameras and computer technology via optical character recognition to automatically read license plate characters and compare digital images to lists of known vehicle information of interest (hot lists).

ALPR Operator

Trained NYSUPD personnel who may search the ALPR system or equipment include the Chief of Police, Lieutenants, Officers, and Dispatchers.

ALPR Administrator

The Chief of Police (or designee) is the ALPR Administrator and is charged with ensuring the ethics and integrity of the process and ensuring that all ALPR operators are appropriately trained.

ALPR Equipment

ALPR cameras including those that are permanently or temporarily affixed in their positions, such as to a structure, pole, or traffic barrier.

ALPR System

The technology system, including ALPR equipment and additional technology services hosted by the ALPR system vendor, that captures images (ALPR data) of a vehicle's characteristics (including license plates) and compares the characteristics to the National Crime Information Center (NCIC) or data entered by law enforcement agencies, which may result in a Hit.

ALPR Data

Captured images produced from the ALPR system. ALPR Data may be downloaded and housed in the University Police secure data repository.

Hit

Alert from the ALPR System that a scanned license plate may be in the National Crime Information Center (NCIC) or other law enforcement database for being related, but not limited to: criminal investigations, stolen or wanted vehicles, stolen license plates, wanted persons, missing/endangered persons, vehicles with known associated exclusions to SUNY Delhi's campus (including any related protection orders), or threats to persons or property.

Hot Lists

Data that includes license plate numbers of stolen vehicles, stolen license plates, and wanted person(s) with a license plate associated with those records. This term also includes, but is not limited to, national data (i.e., NCIC) for similar categories, license plates associated with AMBER alerts or missing persons/ vulnerable adult alerts, and can include manually entered license plate information associated with crimes that have occurred in any local jurisdiction or other investigative targets.

These lists are not tied to the NYS Department of Motor Vehicles and will not include vehicles with administrative issues such as expired or suspended registrations, unpaid fines, etc.