# UW-Madison Police Department

**Policy: 41.16**
**SUBJECT: AUTOMATED LICENSE PLATE READERS (ALPRs)**
**EFFECTIVE DATE: 05/31/24**
**REVISED DATE: 05/16/24; 08/27/24; 12/17/25**
**REVIEWED DATE:**
**STANDARD: CALEA 41.3.9**

**INDEX:**



**POLICY:**

The University of Wisconsin-Madison Police Department utilizes ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. This technology aids in the public safety of students, visitors to campus, and faculty.

All data images gathered by the ALPR/LPR are for the use of University of Wisconsin-Madison Police Department for investigative purposes. Such data may contain confidential information, it is subject to the University of Wisconsin-Madison Police Department's open records policy prior to any release of information.

**DEFINITIONS:**

"ALPRs" refers to Automated License Plate Readers.
"BOLO" refers to alert others about stolen items and or suspicious subjects.
"LPR" Licenses Plate Recognition.
"Hot List" plates that will give alerts on stolen vehicles, known wanted persons, and more.
"UWPD" University of Wisconsin-Madison Police Department.
"Alert" Refers to a notice that is triggered when the LPR system receives a potential "hit" on a license plate.
"Hit" Refers to a result matching a previously registered plate on a "hot list" of stolen vehicles, wanted vehicles, or other factors supporting investigation.
"Flock" refers to Flock Group Incorporated's Flock Safety an ALPR system.

**41.16.1 ADMINISTRATION**

A. The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by UWPD to convert data associated with vehicle license plates for official law enforcement purposes, including 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, and stolen property recovery.

B. Installation and maintenance of the in-car ALPR equipment, as well as ALPR data retention and access, shall be managed by the IT Manager. The IT Manager will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

C. Installation and maintenance of the self-contained ALPR equipment, as well as ALPR data retention and access, shall be managed by Digital Forensic administrators. Digital Forensic administrators, and other approved members of Investigative Services, will administer the day-to-day operation of the ALPR equipment and data.

**41.16.2 OPERATIONS**

Use of all ALPR is restricted to the purposes outlined below, along with the training on the system. Department members shall not use, or allow others to use, the equipment or database records for any purpose other than outlined below.

A. Administrators for each ALPR system shall determine which members of the department are authorized to receive training. All authorized personnel utilizing ALPR equipment or accessing ALPR data shall first complete department approved training.

B. Administrators for each ALPR system shall add authorized users to the agency user list. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation.

C. An ALPR may be used in conjunction with any routine patrol or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

D. Partial License plates reported during major crimes (e.g., homicide, aggravated assault, trafficking, rape) should be entered into the ALPR system to attempt to identify suspect vehicles.

E. If practicable (as outlined in the guidelines for use of both systems below), the authorized users should verify an ALPR response through the TIME System before taking enforcement action that is based on an ALRP alert.

F. An ALPR shall not be used for immigration enforcement, harassment or intimidation, usage based solely on a protected class (i.e., race, sex, religion), or personal use.

G. 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 of the information by name, date, and time.

H. ALPR system audits should be conducted by the system administrators on an annual basis or as needed to identify violations of this policy.

**41.16.3 GUIDELINES FOR USE**

A. Operational guidelines for in-car systems
   i. At the beginning of each patrol officer's shift, they shall log onto the in-car LPR system, it shall remain running in the background throughout an officer's shift
   ii. All patrol squads must run the LPR system in the back ground if the vehicle is equipped.
   iii. Officers shall upon LPR alerts confirm with dispatch the status of the plate in question and provide a response with accompanying comments if needed into the Motorola System.
   iv.

B. Operational guidelines for self-contained systems
   i. All placement and needs-based decisions for the self-contained ALPR systems shall be made by Digital Forensics administrators, with input from Investigative Services, Field Services, and the ALPR team. All purchases of these systems shall be performed by Digital Forensic administrators, with guidance from Finance Team.
   ii. The system must be installed by either a designee from the ALPR team or the manufacturer.
   iii. Maintenance (e.g., camera mounting adjustments, battery replacement, and software updates) shall be performed by a designee from the ALPR team or the manufacturer.
   iv. The primary purpose shall be for Investigative Services. This system is not going to be set to prompt alerts.
   v. All data collected from UWPD-owned ALPR system can be shared with external law enforcement and government agencies that also have the same system in place.
   vi. Data collected from self-contained systems will not be shared with privately owned systems.

**41.16.4 TRAINING**

The ALPR/LPR systems are intended for use by trained employees of the Investigative Services unit, sworn staff, dispatch, and administrators of the system.

A. All authorized users shall complete department training facilitated by an administrator (i.e., Digital Forensics Investigator, Digital Forensic Detective, IT Manager) of the ALPR/LPR systems.

B. All authorized users must be officially signed off and registered with the associated ALPR system as an official user prior to accessing the system.

C. Records of training and a list of all active users shall be retained by the respective ALPR system administrator.

D. All authorized users must be TIME certified.

**41.16.5 Data collection and Retention**

A. The IT Manager is responsible for ensuring the in-car system and processes are in place for collection and retention of ALPR data (180 days minimum). Digital Forensic administrators are responsible for ensuring the self-contained system and processes are in place for collection and retention of ALPR data (30 days maximum, this is set by manufacture not through UWPD). Data that results in law enforcement action, or is utilized as an investigative source, must be archived in accordance with department procedures. All Stored ALPR data should be retained in accordance with the established records retention schedule (Wisconsin Legislature 165.87(3)(c)1.). MOU's with each sharing agency should be maintained and kept for the duration of the system in case of error or wrong doing.

**41.16.6 RELEASING ALPR DATA**

The ALPR data may be shared with requestors through open requests or other law enforcement agencies.

A. External requests (Open records):

a. Requests for records are analyzed on a case-by-case basis to determine whether the record is exempt from disclosure under applicable law, or the public interest served by not making the record public clearly outweighed the public interest served by disclosure. The request is reviewed by the Records Team for both in-car and self-contained systems. Once requests are accepted, the Records Team will contact the appropriate system administrator to obtain the data and perform redactions, as determined by OLA.

b. LPR data is confidential and can be shared only for legitimate state-wide only law enforcement purposes, when required by law, a subpoena or court order, and when such disclosure is required by the Rules of Court governing discovery in criminal matters. Dissemination to a non-law enforcement agency shall be approved by the Chief of Police Prior to disclosure pursuant to the Public Records Law or other requests outside of law enforcement, the Chief of Police shall consider all factors relevant to balancing the public interest in disclosure of a record against the public interest in non-disclosure including whether:

i. Disclosure of LPR data would infringe on the personal privacy of individuals.

ii. Disclosure could affect the perceived character and reputation of an individual.

iii. Aggregated LPR data is uncorroborated and there may be errors in LPR reads of license plates.

iv. Disclosure of a person's location or pattern of travel could heighten the person's vulnerability to theft or physical harm.

v. Disclosure would chill First Amendment rights by diminishing anonymity as the person travels to and from protected activities (protests, religious services, AA meetings, etc.).

vi. Disclosure of aggregated data could result in unsolicited contact of individuals by commercial enterprises.

vii. A record subject often has an enhanced right of access, however, in this instance this data is not associated with persons. Often a vehicle displaying a license plate is not used exclusively by one person or is registered to more than one person.

c. External request (Law enforcement) requestors shall submit a written request for the ALPR data which should include:

i. The name of the agency

ii. Person requesting

iii. Date of request

iv. The time range suspected car came by camera, if known

v. Purpose of information requesting

d. Any approved personnel completing an external request for Flock Safety LPR data shall create a record of the request and produced results, if applicable, on the internal Share Point website on behalf of the requestor.

e. LPR System statistical information, secondary dissemination logs, stored file access logs, audits, and reports to oversight bodies, Commissions, or Committees may be subject to disclosure or partial disclosure.

B. Internal Requests:

a. All internal requests for the Flock Safety system shall be submitted through the form located on the internal Share Point website and include both the reason for the request and the associated case reference number.

i. In the case of exigent circumstances (i.e., serious felonies or active high threat situations) occurring outside of the day shift hours or on the weekend, requestors should contact the Manager on Call (MOC) to get the request fulfilled by the Detective on Call (DOC). In this specific instance, the DOC shall complete the request form on the internal Share Point website on behalf of the requestor.

b. All internal requests for Motorola can be done through day to day operations by all trained agency staff listed in 41.16.4. Motorola will log and accounts for every search through the system. A request through SharePoint can be made if an officer prefers.

C. All requests, internal and external, shall be retained for two years regardless of approval.