Lake City Police Department

Automated License Plate Reader (ALPR) Policy

Purpose

This policy sets clear standards for the use, management, access, and security of Automated License Plate Reader (ALPR) technology by the Lake City Police Department, as required by Minnesota law. Its purpose is to support legitimate law enforcement investigations while protecting data privacy and public trust.

What is an ALPR?

An Automated License Plate Reader (ALPR) is an electronic system that can record or photograph a vehicle and its license plate, then check that information against law enforcement databases. ALPR systems can be mounted on patrol vehicles or set up in fixed locations.

What Data is Collected

Lake City Police ALPRs may only collect:

- License plate numbers
- Date, time, and location of each vehicle detected
- Images of vehicle license plates, vehicles, and areas near vehicles

Collection of any other data is not allowed.

How ALPR Data is Classified and Used

- All data collected by ALPR is private data or nonpublic data, unless it becomes public as part of an active investigation or under specific exceptions in state law.
- ALPR data may only be compared to the Minnesota license plate database, or to additional data sources if those are part of an active criminal investigation.
- Centralized, statewide repositories for ALPR data are not allowed unless specifically authorized by law.

- ALPRs must not be used to monitor or track individuals except as part of an active criminal investigation and with a warrant, unless there are urgent circumstances.

Data Retention and Destruction

- ALPR data not related to an active criminal investigation must be deleted no later than 60 days after collection.
- If a person facing criminal charges requests that ALPR data be preserved because it might be exculpatory, the data must be kept until the case is resolved.
- Participants in the Safe at Home program (address confidentiality) may request immediate destruction of any ALPR data related to them, unless it is part of an active investigation.
- ALPR data part of an inactive investigation will be destroyed according to the official city and state retention schedule.

Data Sharing

- ALPR data can be shared with another law enforcement agency only if it meets the required standards for access and documentation.
- Sharing must be documented, and the receiving agency must follow all data privacy and security laws.
- ALPR data not related to an active investigation may not be shared with other individuals or organizations, unless specifically allowed by law.

Access Logs and Auditing

- The department must keep a public log showing when and where each ALPR is used, how many plates were recorded, which databases the data was compared to, and the categories of alerts received.
- The department must keep a list of the installation sites and movement dates for all stationary ALPRs and make it available to the public unless classified as security information.

- All accesses to ALPR data must be logged with date, time, purpose, and who accessed the data.
- Every two years, an independent audit must be completed to check compliance, data classification, use, and destruction. The audit is public and failure to comply may result in suspension of the ALPR program.

Internal Access Controls

- Only department members authorized in writing by the Chief of Police (or designee) may access ALPR data, and only for a legitimate, documented law enforcement purpose.
- Every time ALPR data is accessed, there must be reasonable suspicion that the data is relevant to an active investigation, and the access must be properly recorded.
- Access to ALPR data is limited through role-based controls according to staff duties and training.

Reporting Requirements

- The department will notify the Bureau of Criminal Apprehension within ten days whenever a new ALPR system is installed, moved, or integrated with another surveillance device.
- The Bureau will keep a public list of all agencies using ALPRs and their fixed locations unless considered security information.

Penalties

- Willful misuse or unauthorized access to ALPR data or violation of this policy is a crime and may result in a misdemeanor charge.
- Employees who violate this policy are subject to disciplinary action, up to and including suspension without pay or dismissal.

Training and Review

All staff using, managing, or accessing ALPR data will be trained on proper use, data privacy laws, and penalties for misuse. This policy will be reviewed and updated whenever state or federal law changes, or as needed by the Chief of Police.

This policy is mandatory for all Lake City Police Department members. Questions should be referred to a supervisor or the Chief of Police.