FERNDALE POLICE DEPARTMENT	Automated License Plate Reader		
	Date of Issue: June 29, 2023	Effective Date: June 29, 2023	Number: ARTICLE 93
	Reviewed: February 15, 2024	Revision Dates:	
	Distribution: All Department Personnel		Standard: N/A

1.0 PURPOSE

1.1 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 to solve crime.

2.0 POLICY

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Ferndale Police Department to link data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. ALPRs may also be used to gather information related to active warrants, homeland security advisories and bulletins, electronic surveillance, suspect interdiction, and stolen property recovery. It is the intent of the Department to ensure that the access and use of ALPR data is consistent with respect for individuals' privacy and civil liberties. It is also the policy of the Ferndale Police Department not to contribute to the criminalization of poverty. As such, ALPR technology will not be used for traffic enforcement, or the enforcement of civil judgements and immigration laws.

3.0 DEFINITIONS

Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.

ALPR Operator: Trained Department members who may utilize the ALPR system.

ALPR Administrator: The Chief of Police or his designee(s) serve as the ALPR Administrator for the department.

Alert: An audible or visual signal activated upon the recognition of a license plate by the ALPR system.

Detection: Data obtained by an ALPR of an image, such as a license plate, within public view that was read by a device (vehicle description on which it displayed and plate) and information regarding the location of the ALPR system.

Hot List: Data files extracted from the law enforcement databases including, but not limited to, NCIC, SOS, LEIN, and Local police department BOLO's. These data extracts are facilitated numerous times per day in an effort to provide current data.

Hit: Alert from the ALPR system that a scanned license plate number may be in a law enforcement database for a specific reason, but not limited to, relation to a stolen vehicle, wanted person or vehicle, missing person, domestic violation protective order, or terrorist-related activity.

Vehicles of Interest: Including, but not limited to, vehicles that are reported as stolen, display stolen license plates or tags, vehicles linked to missing and/or wanted persons, and vehicles flagged by the Secretary of State Administration or a law enforcement agency.

4.0 OPERATIONAL PROCEDURES

4.1 Administration

The ALPR, also known as License Plate Recognition, allows for automated detection of license plates along with vehicle make, model, color, and unique identifiers through the vendor's vehicle identification technology.

4.1.1 The technology is used by the Ferndale Police Department to convert data associated with vehicle license plates and descriptions for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and/or missing persons. It may also gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

4.1.2 All installation and maintenance of ALPR equipment, as well as data retention and access, shall be managed by the Chief of Police and/or their designee. The Chief of Police or their designee will assign members under their command to administer the daily operations of the ALPR equipment and data.

4.2 ALPR Administrator

The Chief of Police or their designee shall be responsible for compliance with the requirements of Civil Codes and or Laws. The Chief has designated the Detective Bureau Commander as the Department's ALPR Administrator.

4.2.1 Only trained sworn officers and police dispatchers are allowed access to the ALPR system or collect ALPR information.

4.2.2 Ensure that training requirements are completed for authorized users.

4.2.3 ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.

4.3 Operations

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow to use, the equipment or database records for any unauthorized purpose(s).

4.3.1 An ALPR shall only be used for official law enforcement business.

4.3.2 An ALPR shall only be used in conjunction with any patrol operation or criminal investigation; reasonable suspicion or probable cause are not required before using the ALPR.

4.3.3 Partial license plates and unique vehicle descriptions reported during a major crime should be entered into the ALPR system in an attempt to identify suspect vehicles.

4.3.4 No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

4.3.5 The officer shall verify an ALPR response through the Law Enforcement Identification Network (LEIN) before taking enforcement action that is based solely on the ALPR alert.

4.3.5.1 Once an alert is received, the operator shall confirm that the observed license plate from the system matches the actual license plate of the observed vehicle.

4.3.5.2 Before any law enforcement action is taken because of an ALPR alert, the alert shall be verified through a LEIN inquiry by MDC or through Dispatch.

4.3.5.3 Officers shall not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated.

4.3.5.4 ALPR alerts may relate to a vehicle and not the person operating the vehicle; officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle.

For example: if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually match the driver’s description of the wanted subject prior to making the stop or should have another legal basis for the stop.

4.4 Hotlists

An alert alone shall not be the basis for police action. Prior to initiation of a

stop of the vehicle or other intervention based on an alert, department employees shall undertake the following:

4.4.1 Verification of status on a Hot List: An officer must receive confirmation through a LEIN inquiry by MDC or through Dispatch that the license plate was entered as stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

4.4.2 Visual verification of license plate number: Officers shall visually verify that the license plate of interest matches with the image of the license plate captured by the ALPR system, including both alphanumeric characters of the license plate, state of issue, and the vehicle descriptors prior to proceeding.

4.4.2.1 Department employees alerted to a Hot List hit are required to make a reasonable effort to confirm that a wanted person is in the vehicle and/or that a reasonable basis exists before a reasonable stop of the vehicle.

4.4.3 All entries and updates of specific Hot Lists within the ALPR system will be documented by the employee entering or by the requesting department employee within the subsequent incident report or call for service. Hotlist entries and updates shall be approved by a supervisor before entry into the ALPR system.

4.4.3.1 The hits from these data sources should be viewed as informational, created solely to bring the officers' attention to specific vehicles that may be associated with criminal activity.

4.4.3.2 All plates and suspect information entered into the ALPR system Hot List shall contain the following information:

- Entering Department employee's name
- Related case number
- Short synopsis describing the nature of the originating call

4.5 Monitoring Operations
Dispatchers shall ensure that the Flock Safety application is active in the telecommunication center and that the current on-duty dispatcher is signed into the system.

4.5.1 Dispatchers shall monitor the system for any Hot List alerts. Dispatchers should immediately, or as soon as practical, broadcast a BOLO for any of the following Hot List alerts:

- Stolen Vehicle
- Stolen License Plate
- Amber Alerts/Missing children

- Involuntary Missing People

4.5.2 In order to confirm the Hot List alert, dispatch shall run the license plate of the vehicle through LEIN/SOS/NCIC. Dispatch should then broadcast any information gained from the law enforcement systems.

4.5.3 While on patrol, Officers shall ensure that the Flock Safety application is active on their MDC and that they are logged into the system. Officers shall monitor the Flock Safety application for Hot List alerts and respond to those alerts appropriately when available.

5.0 TRAINING
It is the Training Lieutenant's responsibility to ensure that all authorized employees receive department approved training to use or access the ALPR system. No employee shall operate the ALPR equipment or access the data without the approved training.

6.0 LOGIN/LOG OUT PROCEDURE
To facilitate oversight of the ALPR system, all users are required to have individual credentials for access and use of the system and/or data. All investigative inquiries are logged by user and available for auditing and review by the Ferndale Police Department.

7.0 IMPERMISSBLE USES
The ALPR system, and all data collected, is the property of the Ferndale Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this policy.

7.1 The following uses of the ALPR system are specifically prohibited:

7.1.1 **Invasion of Privacy:** Except when done pursuant to a court order such as a search warrant, it is violation of this policy to utilize the ALPR to record license plates except those of vehicles that are visible to public view.

7.1.1.2 Vehicles visible to public view are on a public road or highway, in a place where members of the public have access, such as parking lots or business establishments.

7.1.2 **Harassment or Intimidation:** It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.

7.1.3 Use based on a protected characteristic: It is a violation of this policy to use the ALPR system or associated files or hot lists solely because of a person's or groups race, gender religious or political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

7.1.4 **Personal Use:** It is a violation of this policy to use the ALPR system or associated files or hot lists for any personal use. All personnel are specifically prohibited from making a copy, such as but not limited to, using personal cellular phones, in any format of any video, audio or still photograph generated from the ALPR application or associated files or hotlists for personal use.

7.1.5 **First Amendment Rights:** It is a violation of this policy to use the ALPR system or associated files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

7.1.6 **Immigration Enforcement:** It is a violation of this policy to use the ALPR system for enforcement of immigration laws.

7.1.7 **Traffic Enforcement, Civil Infractions, and Civil Judgements:** It is a violation of this policy to use the ALPR system for traffic enforcement, or the enforcement of civil infractions and civil judgements.

7.2 Any employee who engages in or allows the impermissible use of the ALPR system or the associated files or hot lists may be subject to:

- Criminal Prosecution
- Civil Liability
- Discipline, up to and including termination.

8.0 DATA COLLECTION AND RETENTION

The Chief of Police and/or their designee is responsible for enacting the procedure for proper collection and retention of ALPR data. Data will be transferred to the designated storage in accordance with departmental procedures for report writing, investigations, and evidence procedures.

8.1 All ALPR data downloaded to the server shall be stored in accordance with the established records retention schedule.

8.1.1 ALPR data shall be purged unless it has become, or it is reasonable to become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data shall be uploaded to the evidence drive and documented in the related incident report.

8.2 The ALPR's vendor will store the data and ensure proper maintenance and security of the data stored in their data towers. Recordings not relevant to an active investigation, a formal complaint against this agency, or an officer of this agency must be kept the date it was created plus thirty days.[1]

[1] State of Michigan General Retention Schedule #11 Local Law Enforcement 11.057 - Audio and Video Recordings

8.2.1 Recordings that contain evidence of incidents are retained until the case is solved, closed, and litigation ends. [MCL 780.316]

9.0 ACCOUNTABILITY

All data shall be closely safeguarded and protected by both procedural and technological means.

9.1 The Ferndale Police Department shall observe the following safeguards regarding access to and use of stored data:

9.1.1 All ALPR data downloaded to the mobile workstation shall be accessible only through a login/password-protected system capable of documenting all access information by name, date, and time.

9.1.2 Employees approved to access the ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

9.1.3 Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes.

9.1.4 Every ALPR Detection Browsing Inquiry must be documented by the associated Ferndale Police Department incident report and the reason for the inquiry.

9.1.5 Every ALPR search or hotlist alert that produces investigative leads shall be documented using the outcome-tracking software provided by the ALPR system.

10.0 ALPR DETECTION BROWSING AUDITS

It is the responsibility of the Chief of Police or their designee to conduct an annual audit of the ALPR detection browsing inquiries, including an audit sampling of the ALPR system utilization from the previous 12 months to verify proper use in accordance with the authorized uses of the system. The audit shall randomly select a substantial sampling of the inquiries and determine if each inquiry meets the requirements established by policy.

10.1 The audit shall be documented in an internal report to the Chief of Police. The report shall include any data errors found and any violations of this policy.

11.0 RELEASING ALPR DATA

All non-law enforcement requests for access to stored ALPR data shall be processed in accordance with applicable law and FOIA procedures. The ALPR data may be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

11.1 The procedure for such a request is as follows:

11.1.1 Partnering law enforcement agencies may be granted access to the ALPR system by the Chief of Police or their designee upon meeting the following conditions:

11.1.1.1 The partnering law enforcement agency must have a policy regarding ALPR system usage that contains oversight and accountability provisions consistent with this policy or have a signed memorandum of understanding with this department.

11.1.1.2 A list of approved partnering law enforcement agencies will be documented in the department's electronic files.

11.1.2 A non-sharing law enforcement agency requesting ALPR data must include the agency name, the name of the requesting employee, the incident report related to the request, and a synopsis of the incident. Any investigative aid provided by an FPD member to a non-sharing law enforcement agency will be detailed in an Assist Other Law Enforcement (ALE) incident report.

11.1.3 The request is reviewed by the Chief of Police or their designee.

11.1.4 The approved request shall be documented and retained in the report writing system.

11.1.5 All non-law enforcement or non-prosecutorial agencies will be processed by the FOIA retention schedule.



Dennis M. Emmi
Chief of Police