Hilliard Division of Police Policy Manual	Policy 426
Subject: Automatic License Plate Reader (ALPR)	
Standard Reference:	
Effective Date: September 29, 2021	**Last Revision Date:** June 1, 2023
Approved By: Chief Michael Woods	

Automated License Plate Readers (ALPR)

426.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. The Hilliard Division of Police uses ALPRs 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. The ALPR may also be used to gather information related to active criminal investigations, warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

426.2 DEFINITIONS

A. Alert: Also known as a "Hit" - A positive indication, by visual and/or audible signal, of a potential match between data on the "Hot List" and a license plate scanned by the ALPR system. An alert or "Hit" is NOT conclusive confirmation that a license plate is wanted, and additional investigation is always warranted when an alert is indicated.

B. ALPR Coordinator – Designee of the Chief of Police who will conduct annual or more frequent auditing and reporting of ALPR use and effectiveness to the Chief of Police.

C. Automated License Plate Reader (ALPR) - A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest. ALPR's may be deployed in different configurations including fixed (permanent or semi-permanent installation at specific location) and mobile (attached to a vehicle or trailer). Both configurations operate in the same manner.

D. Fixed Location ALPR (FLOCK System) - Fixed ALPR locations use cameras that are engineered to focus on the rear license plate of vehicles passing by the camera location. The camera images are sent by cellular data signal to an off-site server where the images are compared with license plates from NCIC and local hot lists. License plates that match an NCIC entry or hot list trigger an alert to the user who is logged in to monitor the ALPR system. Although all plates are imaged, only the NCIC entered or hot list plates trigger an alert. The images of the license plates of vehicles passing by the camera are retained for no longer than 30-days.

E. Hot List - License plates associated with vehicles of interest from an associated database, including, but not limited to, NCIC, DMV, Local BOLOs, etc.

F. Mobile ALPR - Mobile ALPR systems work in the same manner as a fixed ALPR. The cameras may be mounted on a vehicle or on a mobile trailer and can be placed in locations of investigative interest. The camera images are captured and cross-referenced in the same manner.

G. Scan File - Data obtained by an ALPR of license plates within public view that were read by the device, including potential images of the plate and vehicle on which it was displayed, and information regarding the location of the fixed or mobile camera position at the time of the ALPR read. Information stored includes a photo of the registration plate showing the rear of the vehicle, a date and time stamp of when the registration plate was read by the ALPR and a GPS coordinate to identify the location the registration plate was read by the ALPR.

426.3 ADMINISTRATION OF ALPR DATA

The Investigations Bureau Commander is designated as the ALPR Coordinator and manages the operation of ALPR equipment and access to data.

426.4 ALPR OPERATION

A. Division use of ALPR is restricted to the purposes outlined below. Division personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

1. An ALPR shall only be used for official and legitimate law enforcement business.
2. An ALPR may be used in conjunction with any official Division investigation. Reasonable suspicion or probable cause is not necessary before using ALPR.
3. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings, and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
4. No member of this division shall operate ALPR equipment or access ALPR data without first completing division-approved training.
5. Officers should verify an ALPR alert through LEADS before taking enforcement action that is based solely upon the ALPR alert.
6. Access to Ohio Law Enforcement Automated Data System (LEADS) data, when used in conjunction with ALPR date is subject to all LEADS access regulations.

426.5 ALPR DATA COLLECTION AND RETENTION

A. All data and images gathered by an ALPR are for the official use of the Hilliard Division of Police.

B. LEADS data containing active NCIC records may be uploaded to the ALPR database on a regular basis. Because such data may contain confidential information, LEADS data is not open to public review.

C. ALPR information gathered and retained by the Division may be used and shared with prosecutors or other criminal justice agencies only as permitted by law.

D. ALPR data that becomes part of an investigation or criminal or civil action shall be downloaded to Division storage devices and retained in compliance with the Division's Records Retention Schedule.

E. Local alerts can only be entered into the ALPR system with authorization from a supervisor.

426.5.1 FLOCK STORAGE AND RETENTION

A. FLOCK Group, Inc., the ALPR vendor, will store the ALPR data (data hosting) for no longer than 30 days and ensure proper maintenance and security of data stored in their cloud-based system. FLOCK will also oversee purging data at the end of the 30-day storage period. The Division is responsible for extracting, downloading, and archiving footage from FLOCK on its own storage devices for auditing, prosecutorial and administrative purposes.

B. All ALPR data is encrypted in transit from camera to cloud storage and encrypted at rest in the cloud.

C. Information gathered or collected, and records retained by the FLOCK Safety system on behalf of the Division, will not be:

1. Sold, published, exchanged, or disclosed for commercial purposes.
2. Disclosed or published without authorization.
3. Disseminated to persons not authorized to access or use the information.

426.6 ACCOUNTABILITY AND SAFEGUARDS

A. All saved data will be closely safeguarded and protected by both procedural and technological means. The Hilliard Division of Police will observe the following safeguards regarding access to and use of stored data:

1. All non-law enforcement requests for access to ALPR data shall be referred to the Investigative Bureau Commander and processed in accordance with applicable law.
2. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access to information by name, date, and time.

3. Division members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only. The corresponding incident or case number shall be entered into the ALPR system when conducting a search of the data.
4. ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes (see procedure included in 426.6.1.D.
5. The Investigations Bureau Commander should conduct quarterly ALPR system access audits.
6. The Investigative Bureau Commander shall purge expired local alerts at least every 60 days.

426.6.1 DATA SECURITY AND ACCESS

A. Access to the FLOCK ALPR systems is achieved through individualized login to FLOCK's web-based server. Once logged in, officers are able to receive hotlists and alerts within the system and can view and search for data. Officers are required to enter a search reason for auditing purposes.

B. All logins and queries will be stored and monitored including:

1. Username
2. Date
3. Time
4. Purpose of query
5. License plate and other elements used to query the system.

C. The Investigations Bureau Commander should conduct quarterly audits to ensure access was made by authorized persons for legitimate purposes.

D. ALPR data is considered a record of a criminal investigation and is confidential and not public record. Data shall not be disclosed outside of the Division except for safety purposes pursuant to a written or electronic request from another requesting law enforcement agency. The request must indicate the agency's incident number and why the agency is requesting the ALPR data, i.e., missing person, wanted subject, stolen vehicle, etc. A Division Watch Commander is authorized to release the requested information after reviewing and approving the request. The search for this information will use the requesting agency's incident number as the search reason. The written or electronic request, along with the approval or denial, will then be forwarded to the ALPR Coordinator for filing.