

Automated License Plate Readers (ALPR) & Flock Safety

435.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, including the Flock Safety system, automatically captures and converts license-plate and vehicle information visible from public locations into searchable data. The Girard Police Department uses ALPR technology only for legitimate law-enforcement and public-safety purposes and to provide real-time intelligence to sworn officers of the Girard Police Department to sustain and enhance officer safety.

Authorized purposes of ALPR technology include identifying stolen or wanted vehicles and license plates; locating missing, endangered, or wanted persons; identifying suspect vehicles; investigating criminal activity; recovering stolen property; criminal interdiction; and other official law-enforcement activities permitted by law and departmental policy.

The Department shall administer ALPR access and data in a manner consistent with the law, individual privacy, civil liberties, constitutional protections, CJIS requirements, and the Department's obligation to maintain public trust.

435.2 DEFINITIONS

ALPR: A camera and related software that automatically captures images of vehicles or license plates and converts the information into searchable data.

Alert: A notification generated when a captured plate or vehicle characteristic potentially matches an entry in a law-enforcement database or custom hot list.

Audit Assistance: A specific Flock Safety function that identifies activity requiring administrative review or validation.

Custom hot list: A Department-created list of license plates or vehicles of interest entered for an authorized law-enforcement purpose.

Historical search: A search of previously collected ALPR data.

Search reason: The documented official purpose for accessing ALPR data, including an associated CAD, incident, report, case, or requesting-agency reference number when available.

435.3 ADMINISTRATION AND RESPONSIBILITY

Flock Safety provides the Department's ALPR equipment, software, data hosting, installation, and maintenance services. The Chief of Police and authorized designees, to include the Administrative Captain and Patrol Captain, shall oversee the Department's ALPR program and shall be responsible for compliance with this policy, applicable law, CJIS requirements, and records-retention obligations.

The program administrators shall:

Girard Police Department

Policy Manual

Automated License Plate Readers (ALPR) & Flock Safety

- Approve, modify, and revoke user access based on assignment and operational need.
- Ensure that users complete Department-approved training before receiving full access to the ALPR system.
- Review system permissions and remove access when a member separates, changes assignment, or no longer has an operational need.
- Coordinate outside-agency access and data-sharing requests.
- Conduct routine audits of the access, use and operation of the ALPR system.
- Ensure required audits, compliance reviews, and retention practices are completed.

435.4 AUTHORIZED USERS

Full access may be granted only to sworn Department members, dispatchers, and other specifically authorized personnel whose official duties require ALPR access. ALPR information shall not be accessed in violation of any law, order, regulation, user agreement, Girard Police Department policy, or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access (OAC § 4501:2-10-03).

All users shall access the system only through their own assigned credentials and shall not share passwords, authentication methods, or active sessions. Departmental members shall immediately report unauthorized access or use of computers, devices, software or systems associated with the ALPR system by another member to their supervisors or Shift Sergeants.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures related to the ALPR system unless directed to do so by a supervisor.

Access shall be limited to the permissions reasonably necessary for the user's assignment. Members shall immediately report suspected credential compromise, unauthorized access, or inappropriate use through the chain of command.

435.5 OUTSIDE-AGENCY ACCESS AND REQUESTS

The Chief of Police or designee may grant ALPR camera or data access to another state or local Ohio law-enforcement agency for an official law-enforcement purpose and as permitted by law. Access may be limited by geography, duration, camera, investigation, or other appropriate conditions.

Requests from state or local agencies outside Ohio shall be evaluated individually and ordinarily limited to the duration and scope of the identified investigation. Access may be denied, restricted, suspended, or revoked when necessary to protect an investigation, comply with law, address misuse, or protect Department systems and data.

Girard Police Department

Policy Manual

Automated License Plate Readers (ALPR) & Flock Safety

When a Department member conducts a search for another agency, the requesting agency's CAD, report, incident, or case number shall be entered as the search reason when available. The requesting agency and requesting member should also be identified when supported by the system.

435.6 AUTHORIZED OPERATION AND USE

ALPR equipment, Flock Safety software, alerts, images, and historical data shall be used only for official law-enforcement or public-safety purposes. **The Girard Police Department shall maintain a seven (7) day data retention policy with its use of ALPR systems in the interest of privacy and investigative practicality.**

Any detention, stop, search, seizure, or other enforcement action of which ALPR equipment, software, alerts, images or historical data is involved with must be independently lawful and consistent with this policy. An ALPR alert is an investigative lead and does not independently establish reasonable suspicion or probable cause. Before taking enforcement action that restricts a person's freedom, members shall take reasonable steps to confirm that the alert is current, accurate, and associated with the observed vehicle.

Verification shall include, as applicable:

- Confirming through LEADS, NCIC, and dispatch that the registration, vehicle, person, warrant, or other entry remains valid and actionable.
- Visually comparing the captured and observed license plates, including the alphanumeric characters, issuing state, plate type when visible, and available vehicle descriptors.
- When the alert concerns only the registered owner, attempting to compare the driver with the wanted person's description and establishing a lawful basis for the stop.
- Considering the warrant pickup radius, entry limitations, partial-VIN matches, plate-reader error, vehicle transfers, stolen-plate circumstances, and other information affecting the alert's validity.

Exigent circumstances may affect the sequence or timing of verification, but members shall complete verification as soon as practical. The reason for any action taken before full verification shall be documented.

Authorized uses of the ALPR system include:

- Routine patrol operations and criminal investigations.
- Locating stolen, wanted, or suspect vehicles and stolen license plates.
- Locating missing, endangered, abducted, or wanted persons.
- Developing leads from full or partial license plates and distinguishing vehicle characteristics reported during criminal activity.
- Supporting task-force, intelligence, interdiction, or court-authorized operations.
- Responding to requests from other law-enforcement agencies for official purposes.
- Preserving relevant ALPR images and information as evidence in a case file.

Automated License Plate Readers (ALPR) & Flock Safety

435.7 TRAINING

No member shall access or operate the ALPR system until completing Department-approved training. Training shall address authorized and prohibited uses, search-reason documentation, alert verification, evidentiary preservation, data security, privacy and civil-liberties considerations, and audit requirements. Annual refresher training may be required following policy changes, system changes, identified misuse, or audit findings.

435.8 SEARCH REASON DOCUMENTATION & PROCEDURE

Each time a member uses a Search, Lookup, or comparable historical-query function, the member shall enter a specific and accurate search reason.

The following will constitute as procedure for conducting a search or lookup function:

- **ALL** applicable offense types shall be entered into the Offense Type field.
- When the activity relates to a **documented event (as supported by a CAD entry, incident entry, or other documentation as created by the Girard 911 Center)**, the member shall enter the associated Girard CAD call number, and/or a Girard incident, report, or case number. A generic description shall not replace an available reference number.
- When a reference number does not yet exist or cannot reasonably be used because of an active or sensitive operation, the member shall maintain sufficient information to identify the authorized purpose, unit, task force, or requesting agency. The activity remains subject to audit and later verification.
- Searches of ALPR data will be limited to the following reasons, of which will be selected in the Reason field:
 - Misdemeanor Criminal Investigations
 - Felony Criminal Investigations
 - Traffic Investigations
 - Wanted Person Investigations
 - Endangered Person Investigations

435.9 PROHIBITED USES

Members shall not use ALPR equipment, software, data, alerts, or hot lists for any of the following:

Unauthorized surveillance or invasion of privacy: Capturing or using ALPR information outside a lawful, official purpose. Unless authorized by a court order, warrant, or other lawful authority, ALPR cameras shall capture only vehicles exposed to public view, including vehicles on public roadways or visible from a public roadway or publicly accessible place.

Harassment or intimidation: Targeting an individual or group to harass, intimidate, retaliate, or otherwise act outside an official purpose.

Automated License Plate Readers (ALPR) & Flock Safety

Protected characteristics: Using ALPR information or hot lists solely because of race, color, national origin, ethnicity, religion, sex, gender, sexual orientation, disability, veteran status, political affiliation, or another classification protected by law.

Personal, commercial, or political use: Using the system for curiosity, personal relationships, private disputes, commercial advantage, election activity, or any non-law-enforcement purpose.

Constitutionally protected activity: Using ALPR information for the purpose or known effect of infringing First Amendment activity or any other constitutional right, absent a lawful and articulable public-safety or investigative purpose.

Credential or data misuse: Sharing credentials, permitting unauthorized access, falsifying a search reason, altering audit information, improperly disseminating data, or attempting to avoid auditing.

435.10 HOT-LIST ALERTS AND ENFORCEMENT RESPONSE

Flock Safety may provide real-time alerts based on LEADS, NCIC, NCMEC, or other authorized law-enforcement databases and Department-created hot lists. On-duty personnel assigned by Department procedure should log in and monitor alerts when operationally practical.

When an alert prompts an officer response, the dispatcher shall create a CAD event if an officer is dispatched, advises that the officer is responding, or begins actively looking for the vehicle. If the dispatcher only broadcasts an alert for general awareness and no officer actively responds, a CAD event is not required unless otherwise directed.

435.11 REQUIRED VERIFICATION

An ALPR alert is an investigative lead and does not independently establish reasonable suspicion or probable cause. Before taking enforcement action that restricts a person's freedom, members shall take reasonable steps to confirm that the alert is current, accurate, and associated with the observed vehicle.

Verification shall include, as applicable:

- Confirming through LEADS, NCIC, or dispatch that the plate, vehicle, person, warrant, or other entry remains valid and actionable.
- Visually comparing the captured and observed license plates, including the alphanumeric characters, issuing state, plate type when visible, and available vehicle descriptors.
- When the alert concerns only the registered owner, attempting to compare the driver with the wanted person's description or establishing another lawful basis for the stop.
- Considering the warrant pickup radius, entry limitations, partial-VIN matches, plate-reader error, vehicle transfers, stolen-plate circumstances, and other information affecting the alert's validity.

Exigent circumstances may affect the sequence or timing of verification, but members shall complete verification as soon as practical. The reason for any action taken before full verification shall be documented.

Automated License Plate Readers (ALPR) & Flock Safety

435.12 INVALID OR SUPPRESSED ALERTS

When an alert is determined to be invalid, dispatch shall promptly notify responding officers. The shift supervisor shall be notified of recurring or clearly invalid alerts, including alerts based on an out-of-radius warrant, a mismatched vehicle, or an incorrect partial-VIN association.

After reviewing the circumstances, an authorized supervisor or administrator may suppress the alert to prevent repeated invalid notifications. Suppression shall not be used to conceal valid activity or defeat an authorized investigation and should be removed when no longer justified.

435.13 CUSTOM HOT-LIST ENTRIES

Custom hot lists in Flock are user-created databases of specific license plates or vehicle descriptions. They trigger real-time alerts when captured by ALPR cameras.

Only personnel authorized by the Chief of Police may create a departmental custom hot-list entry. Any custom hot list entry, notwithstanding exigent circumstances, will be subject to the review, approval, and administration of the Patrol Captain. **Requests for the addition of a registration or vehicle to the departmental custom hot list will be provided directly to the Patrol Captain for review, approval, and subsequent entry.**

Upon order of a turn supervisor, a temporary entry may be made into the departmental custom hot-list by an on-duty dispatcher for exigent circumstances, to include purposes of facilitating real-time intelligence to GPD personnel to help facilitate the capture of a wanted person, the protection of a crime victim, the recovery/provision of aid to an endangered person, or other exigent circumstances. The entry of a hot-list record by dispatch will be documented in the call/CAD notes to include the supervisor of whom ordered the entry, and the time in which it was requested. The use of this type of entry shall be documented as "Temporary Exigent Circumstances", will be accompanied with a call, incident, or report identification number for later review, and be provided directly to the Patrol Captain as soon as practical.

Custom hot-list entries will be supported by an incident report number detailing the reasons for the entry, or in the case of an exigent circumstances, a CAD call number. An internal report number/CAD call number is required for all additions of a registration or vehicle to the departmental custom hot-list. Entries associated with sensitive task-force or intelligence operations may be confirmed through the appropriate liaison and Patrol Captain without disclosing operational details beyond what is necessary to establish compliance.

Every entry shall serve a current, legitimate law-enforcement purpose and include enough information to identify the responsible member, associated investigation or event, reason for entry, and expiration or review date when supported by the system.

Every entry of a registration/vehicle into the departmental custom hot-list will be limited to the following reasons, of which will be listed at time of entry:

Automated License Plate Readers (ALPR) & Flock Safety

- Misdemeanor Criminal Investigations
- Felony Criminal Investigations
- Traffic Investigations
- Wanted Person Investigations
- Endangered Person Investigations
- Temporary Exigent Circumstances

The Patrol Captain shall promptly remove an entry when the vehicle is no longer wanted, the investigative need has ended, the information is no longer reliable or continued alerting no longer serves a reasonable purpose. Officers who have made a request for a custom hot-list entry will further update the Patrol Captain regularly about the status of an approved entry to determine if the entry should be removed, updated, or otherwise altered.

The Patrol Captain shall review custom hot-list entries every thirty (30) days, and in the event of an Temporary Exigent Circumstance, within five (5) days. Stale, unsupported, duplicative, or unnecessary entries shall be removed by the Patrol Captain upon their review.

435.14 DATA COLLECTION, SECURITY, AND RETENTION

Flock Safety hosts ALPR data and is responsible for maintaining the security and operation of data stored on its systems consistent with the Department's agreement. Per GPD's agreement with Flock Safety, Flock shall automatically purge collected ALPR data after 7 days.

The automatic purge does not prohibit the Department from preserving relevant ALPR information for an authorized investigation, prosecution, public-records obligation, litigation hold, audit, training review, or other lawful purpose.

435.15 EVIDENTIARY PRESERVATION

When ALPR information is used to investigate or prosecute an offense, the responsible member shall download and preserve relevant images, vehicle information, maps, timestamps, search results, and related information in the applicable report, evidence system, or case file before the vendor's retention period expires. Preserved information shall be retained in accordance with the City's records-retention schedule and applicable evidentiary requirements.

435.16 ACCESS, DISCLOSURE, AND SALE

ALPR information shall not be sold or used for any purpose other than legitimate law-enforcement or public-safety activity. Members shall not disclose ALPR information outside authorized channels. Public-records requests, subpoenas, discovery requests, and other demands for ALPR records shall be processed in accordance with law and Department procedure, with

Automated License Plate Readers (ALPR) & Flock Safety

appropriate review for confidential law-enforcement investigatory records, security records, personal information, and other protected material.

435.17 AUDITING AND COMPLIANCE REVIEW

The Department shall regularly audit ALPR activity, at least quarterly, to ensure compliance with this policy, Department procedures, applicable law, and CJIS standards. Audit findings may be used to identify training needs, access-control changes, policy revisions, corrective action, or further investigation.

435.18 AUDIT ASSISTANCE REVIEW

All auditable activity reported through Flock Safety's Audit Assistance function shall be individually hand-audited. Every reported instance shall be exported as a CSV file, printed, and reviewed by the Chief of Police and/or Patrol Captain. Instances of suspected misuse or abuse of the ALPR system or violations of this policy will also be hand-audited following this same procedure.

The reviewer shall complete the following process:

1. Review the Audit Assistance entry, including the user, date and time, search type, stated reason, search parameters, and available audit history.
2. Search Sundance using the associated CAD call, incident, report, or case number to determine whether the activity was connected to a documented law-enforcement purpose.
3. If the stated number does not substantiate the activity, search Sundance using the queried license plate or vehicle-registration information.
4. If no associated record is located, review call files, calls for service, incident reports, and case records from the date of the Flock activity for a legitimate connection to the queried plate or vehicle.
5. When the activity may involve a wanted person or warrant investigation, consult the publicly accessible Girard Municipal Court records for historical warrant or wanted-person information that may substantiate the activity.
6. Refer registration or license-plate checks associated with task-force operations to the appropriate Department task-force liaison or task-force member. The liaison or member shall investigate and confirm whether the activity was conducted for an authorized, legitimate law-enforcement purpose. Operationally sensitive information need not be placed in the general audit record, but the confirmation and sufficient information to establish compliance shall be documented.
7. If the activity remains unverified, manually review the plate, vehicle information, search circumstances, related internal records, and any other available information, and commence further internal investigation when necessary.
8. Refer activity that cannot be substantiated or appears inconsistent with policy, procedure, CJIS standards, or law for further internal investigation and document the referral in accordance with Department procedure.

Girard Police Department

Policy Manual

Automated License Plate Readers (ALPR) & Flock Safety

435.19 AUDIT DOCUMENTATION AND CONFIDENTIALITY

The exported CSV file, printed Audit Assistance report, supporting records, reviewer findings, task-force confirmation, and any resulting investigative documentation shall be maintained in accordance with the City's records-retention schedule.

Audit records containing confidential investigations, criminal-intelligence information, task-force information, protected personal information, security information, or CJIS data shall be stored with access restrictions appropriate to the information. Audit documentation shall contain enough information to establish compliance without unnecessarily exposing sensitive operational details.

435.20 OTHER ADMINISTRATIVE AUDITS

The Chief of Police or designee may conduct additional random, periodic, incident-specific, complaint-based, or user-specific audits. Members shall cooperate with authorized audits and provide requested information. No member shall alter, conceal, destroy, or omit information for the purpose of interfering with an audit or compliance review.

435.21 VIOLATIONS

Suspected misuse, unauthorized access, falsification of a search reason, improper disclosure, failure to preserve required evidence, repeated failure to remove stale hot-list entries, or interference with an audit shall be reported through the chain of command. Violations may result in suspension or revocation of ALPR access, remedial training, administrative investigation, discipline, criminal referral, or other action permitted by law, Department policy, and any applicable collective bargaining agreement.

435.22 POLICY REVIEW

The Chief of Police or designee shall review this policy periodically and following material changes to applicable law, CJIS requirements, vendor functions, Department operations, or identified audit trends. Members shall be notified of substantive changes and complete additional training when directed.