

41. 52 Flock Safety System

This Policy provides Department employees with guidelines on the deployment, data storage, retention, and associated uses of the Flock Safety System.

It is the Policy of the Department that the Flock Safety System and captured data will be used in strict accordance with department policy and procedures, training, and applicable Federal and State law.

The Department does not use Flock Safety System to monitor individuals based solely on race, ethnicity, religion, political affiliation, or other protected characteristics.

Definitions:

Alert: A visual and/or auditory notice that is triggered when the LPR system receives a potential “hit” on a license plate.

Flock Safety System: A system that delivers real-time situational awareness by integrating automated license plate readers, video surveillance, gunshot detection technology, drone as a first responder, and live 911 data to detect, investigate, and respond to incidents.

Hit: A read matched to a license plate previously registered on an agency’s “hot list” of vehicle license plates.

Hot List: A database of license plates or vehicles of interest entered into the Flock Safety system to generate real-time alerts when detected. Hot list entries may originate from sources such as the National Crime Information Center, National Center for Missing and Exploited Children, or be manually entered for legitimate criminal justice and public safety purposes to support investigations conducted by the Casa Grande Police Department or other law enforcement agencies.

LPR: The LPR system is an automated information technology that is both non-discretionary and non-discriminatory, with the efficiency of quick scanning and matching capabilities.

A. General

The Flock Safety System, associated equipment, and databases are authorized for official criminal justice and public safety purposes. Misuse of this equipment and related databases, or data, is prohibited. Any use for personal reasons is strictly prohibited.

The use of Flock Safety System is restricted to this agency's criminal justice and public safety related missions. Flock Safety System, data, and associated media are the property of this agency and intended for use in conducting official business, including department related civil or administrative matters as approved by the Chief of Police.

During the course of an investigation, officers shall discontinue the use of Flock once it has been determined that no further investigative action is necessary or warranted.

B. Administration

1. The Flock Safety System is supervised by the Patrol Deputy Chief. They are responsible for the following:

- a. Annual review of Flock Safety System fixed locations.
- b. Oversee audits of searches, hot lists, user access and permissions.
- c. Operational effectiveness
- d. Ensure personnel receive training in the use of Flock Safety System.
- e. Serve as the point of contact with Flock Safety.

C. Flock Safety System Usage

1. Flock Safety System and access to collected data shall be for official use only.

2. Only sworn personnel or professional staff who have been granted access and trained in the use and operational protocols of the Flock Safety System shall be permitted to use it.

3. At the start of each shift, sworn personnel shall log into the Flock Safety system when their assignment or duties may reasonably benefit from the information it provides.

4. Flock Safety System Alerts/Hits. Before initiation of a vehicle stop, an officer shall:

- a. Visually verify that the vehicle license plate number matches the license plate number provided by the Flock Safety System, including both alphanumeric characters of the license plate and the state of issuance.
- b. Verify the current status of the license plate through MVD query when circumstances allow.
- c. In instances where verified information provided by the Flock Safety System does not, by itself, establish reasonable suspicion for a vehicle stop, the officer shall independently develop reasonable suspicion prior to initiating the stop.

5. In each case where an alert is triggered and the vehicle is apprehended the user shall record the disposition of the alert into the Flock Safety System.

6. Searches of historical data within the Flock Safety system shall be conducted only for criminal justice or public safety purposes and in accordance with all applicable departmental policies and procedures.

a. When conducting a search, the following fields are required to be filled out:

- Offense Type
- Case Number
- Reason

b. The Chief of Police must approve of any searches related to an administrative or internal investigation.

7. Custom Hot Lists may be created by personnel authorized to use the Flock Safety System and shall only be used for official criminal justice or public safety purposes.

a. Personnel adding a license plate to a custom hotlist shall include the following information

- License plate number
- License plate State
- Case number: Department Report (DR), Call for Service (CFS) number or Incident Number shall be used.
- Reason for the hotlist: Ex. Missing person, stolen vehicle, etc.
- Notes: Details related to the reason for adding the vehicle to the hotlist
- Media Files: Not required but may be added.

b. Expiration of Hot List Alerts

- Alerts shall not be created for longer than 30 consecutive days without permission from the employee's supervisor.
- The employee who adds a license plate to a hot list is responsible for removing the license plate when there is no longer a criminal justice or public safety purpose.
- Sergeants / first line supervisors shall check their teams / subordinates Hot Lists once per month to ensure they meet the guidelines set forth in this policy.

8. Gunshot Detection System (GDS):

Officers shall not detain or arrest solely on a GSD alert.

1. The GSD is a lead-only tool. A GSD alert, by itself, does not give the responding officers the legal authority to enter a private residence, private buildings, and/or the constitutional curtilage surrounding these properties.
2. Any possible connection or involvement of any subject to the GSD notification must be determined through further investigation and investigative resources.
3. Any arrest must be based upon probable cause.

D. Data Sharing, Dissemination and Public Records

1. Flock Safety System data shall be treated as confidential information and may be shared with other law enforcement agencies for their legitimate criminal justice or public safety purposes.
2. Flock Safety System data may be shared with the public when it helps advance an active investigation. In these cases, reasonable steps will be taken to protect unrelated information and safeguard the privacy of individuals who are not part of the investigation.
3. Flock Safety System data will not be released to a private citizen, except as may be required by law.

E. Accountability, Audits, and Retention

1. Flock Safety System retains data for 30 days. Data automatically deletes after 30 days.
2. Flock Safety System shall be accessed only through City-owned electronic devices and secured via login/password-protected system, including applicable servers, with the capability to log and document all access to information in accordance with Department and City protocols.
3. Personnel are prohibited from accessing any Flock Safety System using personally owned electronic devices.
4. Retention of any Flock Safety System Data will be stored in Evidence.com or downloaded onto portable media and retained in evidence. They shall be retained as applicable by state records retention laws.
5. Under no circumstances will an unauthorized person be allowed access to the Flock Safety System.
6. User access violations will be subject to Department and City disciplinary action and potential civil or criminal penalties.
7. Division lieutenants are responsible for ensuring that all searches flagged by the Audit Assistant Tool and Sensitive Search Warning Alert are reviewed on a weekly basis. Any searches determined to be outside of policy shall be forwarded through the chain of command to the Chief of Police for final review and disposition.
8. Officers are responsible for auditing and updating their hot lists weekly. Sergeants are responsible for conducting weekly audits of their teams' hot lists, to include any of their own hot lists. Division lieutenants are responsible for ensuring organizational hot list entries are reviewed on a weekly basis for compliance with department policy. Any entries determined to be outside of policy shall be removed.

41.52.1 Real Time Information Center

The mission of the Real Time Information Center (RTIC) is to leverage technology to provide real-time, actionable intelligence that enhances officer and public safety, supports incident response, and assists in identifying patterns to prevent and disrupt crime.

DEFINITIONS:

City-Owned Video System: Any camera, network infrastructure, recording device, or other hardware/software owned and maintained by the City of Casa Grande.

Privately-Owned Video System: Any camera, network infrastructure, recording device, or other hardware/software owned and maintained by a private entity.

Real-Time Information Center (RTIC): A centralized location within the Casa Grande Police Department that uses technology and data analysis to provide immediate, actionable intelligence to officers and investigators in real-time. The Center will also support on-going investigations and enhance situational awareness.

RTIC Operator: Public safety professional responsible for monitoring, analyzing, and disseminating real-time information from integrated public safety technologies to support law enforcement operations, enhance situational awareness, and assist in the detection, investigation, and response to incidents.

COMMAND STRUCTURE

RTIC is part of the Patrol Division and is supervised by the Patrol Division Deputy Chief.

FUNCTIONAL RESPONSIBILITY

1. Provide intelligence sharing and investigative assistance to first responders in real time.
2. RTIC operators monitor video systems, monitor calls for service, operate unmanned aerial System (UAS), and coordinate real-time responses to incidents in support of field personnel and ongoing operations.
3. Collaborate with Public Safety Communications when RTIC is involved in calls for service.
4. Serve as a liaison with other RTICs and provide real-time information to partner agencies requiring Casa Grande Police Department (CGPD) information.

VIDEO NETWORK

A. Description

1. The CGPD video network is comprised of city-owned video systems and other integrated public and private cameras.
2. Access to the CGPD Video Network is limited to RTIC operators and authorized personnel.

B. Privacy Considerations

1. RTIC operators and authorized personnel operate RTIC resources, including the video network, professionally and ethically in conformance with all applicable laws, access agreements, memorandums of understanding (MOU), or intergovernmental agreements (IGA). Data and imagery are only used for law enforcement or public safety purposes or as otherwise required by law.
2. No unauthorized recording, viewing, reproduction, retention, or distribution of video network data is allowed, except as authorized or required by departmental policy or law.
3. Cameras are only used to assist first responders with active calls for service (CFS), investigations, or other lawful purposes.
4. RTIC operators or other authorized personnel will not:
 - Intentionally maneuver private or publicly owned cameras into areas with an expectation of privacy absent exigent circumstances, a search warrant, or the property owner's permission.
 - Absent exigent circumstances or a search warrant, monitor areas where the public has an increased expectation of privacy, such as a private residence or public bathrooms.

C. Private/Public Sector Video Integration

1. All private and outside public entities must have a written Agreement with CGPD authorizing CGPD to access their video system for public safety purposes.
2. Access to the privately-owned video systems is subject to the following provisions:
 - a. Each private entity will provide access enabling RTIC to view and use the video system to gather mission critical intelligence.
 - b. Each entity may specify through the Agreement what cameras RTIC may access (e.g., interior, exterior, etc.).
 - c. Each entity authorizes RTIC to review video applicable to the collection of real-time intelligence for public safety use or investigations.
 - d. RTIC operators may record from the private camera system for law enforcement purposes only.
 - e. It is understood the entity reserves the right to withhold any recordings made by their system, necessitating RTIC personnel or other police personnel to obtain the recordings through a warrant or subpoena.
 - f. RTIC is not a camera monitoring service for the private entity and will only access cameras for active public safety incidents or ongoing investigations.
 - g. RTIC will adhere to the stipulations within the Agreement for using the cameras for public safety needs with deviations occurring only under exigent circumstances with post-incident notifications to the camera system owner to explain such deviation.

ACCESSING CAMERAS on the VIDEO NETWORK

- A. Only RTIC operators or other authorized members of the City of Casa Grande public safety team will access the live footage from video networks.
- B. Live video footage shall be viewed in a manner that safeguards sensitive information and protects privacy. All Department mobile and stationary workstations and servers shall be accessible only through login/password-protected system capable of documenting all access to information in accordance with Department and City protocols.
- C. Control and monitoring of RTIC video networks will be conducted in a professional, ethical, and legal manner.
- D. Video recordings are limited in length by the capabilities of the particular security camera system.
 - Based on public safety needs, only access the pertinent portion of the recorded video to collect real time intelligence.
- E. When RTIC plays an active role in assisting first responders with real-time intelligence, the RTIC operator will document the assist following departmental report writing policy.
- F. When accessing cameras on the network camera owners have primary override control of their cameras.

1. If the private/public entity and an RTIC operator attempt to control the camera simultaneously, the RTIC operator will relinquish control of the camera.
2. In exigent circumstances where access to a camera is critical to the safety of the community or law enforcement personnel, personnel should make reasonable efforts to contact the responsible party to obtain full control of the camera.

VIDEO NETWORK REQUESTS

A. CGPD employees may request RTIC assistance to obtain historical video footage related to cases, incidents, or investigations to which they are assigned or assisting.

1. The requesting employee is responsible for ensuring that the requested video footage is uploaded and submitted to Evidence.com.
2. Requests for historic video footage from schools must be directed through the appropriate school district, not the RTIC.
3. RTIC operators shall be responsible for incidents they have live-viewed and actively participated in, utilizing available footage to provide real-time updates to field units.

B. RTIC and other authorized personnel shall follow Department policy governing the purging and retention of saved video, in accordance with guidelines established by the Arizona Department of Library, Archives, and Public Records.

RTIC UAS OPERATIONS

A. Drone operations will be done in accordance with Policy 41.42 Deployment and Use of small Unmanned Aerial System.