

## **Executive Summary**

The Police Department's Surveillance Technology Policy establishes rules for the use of two law enforcement technologies: **Automatic License Plate Readers (LPRs)** and **Unmanned Aircraft Systems (drones)**.

Both technologies can improve public safety, increase officer safety, assist criminal investigations, and allow officers to respond more efficiently to certain incidents. At the same time, the Department recognizes that these technologies have the potential to collect significant amounts of information and must therefore be subject to clear limitations, oversight, and accountability.

The proposed policy is designed to ensure that LPRs and drones are used only for legitimate and lawful law enforcement purposes and in compliance with North Carolina law, federal law, constitutional protections, and applicable Federal Aviation Administration requirements.

The policy establishes specific restrictions on use, limits access to authorized and trained personnel, requires documentation of certain activities, establishes data-retention and disclosure requirements, provides for supervisory review and auditing, and prohibits the use of the technology for personal, discriminatory, retaliatory, or other unauthorized purposes.

The intent of the policy is to provide the Department with useful public-safety tools while establishing strong safeguards to protect individual privacy and maintain public trust.

## **AUTOMATIC LICENSE PLATE READERS**

### **What is an LPR?**

An Automatic License Plate Reader is a camera system capable of detecting license plates on passing vehicles and converting the license plate image into searchable computer data.

Depending upon the system, the information may include the license plate number, date and time of detection, location of the camera, and an image of the vehicle.

LPR cameras do not determine who is driving the vehicle and do not automatically establish that a person has committed a crime.

### **Why does the Police Department need LPR technology?**

LPR systems can quickly assist officers and investigators in locating vehicles connected to legitimate law enforcement matters.

Examples include:

- Locating stolen vehicles;
- Locating missing or endangered persons;
- Locating vehicles associated with criminal investigations;
- Assisting in the apprehension of persons with qualifying felony warrants;
- Developing investigative leads in criminal cases; and
- Assisting other law enforcement agencies with authorized criminal investigations.

The technology can perform tasks that would otherwise require officers to manually observe and compare hundreds or thousands of license plates.

### **Can LPR cameras be used to issue speeding tickets or other routine traffic citations?**

No.

North Carolina law restricts the use of captured LPR data and specifically prohibits its use for the enforcement of traffic violations.

### **Does an LPR alert automatically give an officer authority to stop or arrest someone?**

No.

Under Department policy, an LPR alert is treated as an investigative lead.

When reasonably practicable, an officer must visually verify the license plate, confirm that the information generating the alert remains valid, compare available vehicle information, and evaluate the totality of the circumstances.

Any detention, arrest, or search must still have the legal justification required by law.

## **Can officers search the LPR database whenever they want?**

No.

Historical searches may only be conducted for an authorized law enforcement purpose.

When supported by the system, the employee conducting the search must identify the associated case or incident and document the reason for the search.

Searching the system because of curiosity or for a personal, political, commercial, retaliatory, or other unauthorized purpose is prohibited.

## **Can LPR technology be used to follow someone's movements?**

The technology may only be used within the purposes authorized by North Carolina law.

The policy places additional restrictions on broad searches intended to identify patterns of movement, associations, or vehicles present at sensitive locations or activities.

Such searches should receive supervisory authorization, and the policy specifically provides heightened protection for constitutionally sensitive locations and activities such as religious institutions, political events, demonstrations, and similar activities.

## **How long is LPR information retained?**

Routine captured plate data may not be preserved for more than **90 days**, except when continued preservation is specifically authorized under North Carolina law.

For example, information that becomes relevant to an active criminal investigation may be preserved through legally authorized procedures.

## **Is LPR data available to the general public?**

No.

North Carolina law classifies captured plate data as confidential and provides that it is not a public record.

The policy also restricts disclosure of the information to persons and agencies authorized by law.

### **Can the Department share LPR information with other agencies?**

Yes, but only under the conditions permitted by North Carolina law.

Requests from qualifying law enforcement agencies must be for an authorized law enforcement purpose and must meet applicable documentation requirements.

The Department maintains records of information disclosures.

### **What prevents an officer from using the system to look up a spouse, neighbor, friend, public official, or other person?**

Several safeguards are built into the policy:

- Access is limited to authorized personnel.
- Employees use individual system credentials.
- Searches may be recorded in system audit logs.
- Historical searches require an authorized law enforcement purpose.
- Case or incident information is documented when supported by the system.
- The Department conducts an ALPR audit at least annually.
- Personal or curiosity-based searches are specifically prohibited.
- Suspected misuse must be reported and investigated.
- Violations may result in disciplinary action and may also carry criminal penalties under North Carolina law.

## **UNMANNED AIRCRAFT SYSTEMS — DRONES**

### **Why does the Police Department need drones?**

A drone can provide officers with information from locations that may otherwise be difficult, dangerous, or time-consuming to access.

Examples of appropriate uses include:

- Searching for missing children, elderly persons, or other endangered persons;

- Search and rescue operations;
- Barricaded-person and hostage situations;
- Tactical incidents;
- Crime scene documentation;
- Serious traffic collision reconstruction;
- Hazardous-material incidents;
- Disaster response;
- Assessing dangerous locations before sending officers or emergency personnel into an area;
- Searching large wooded or difficult-to-access areas; and
- Other legally authorized public-safety operations.

In many situations, a drone may allow the Department to obtain necessary information without unnecessarily placing an officer, firefighter, or member of the public in danger.

### **Does having a drone mean the Police Department can fly over private property and conduct surveillance whenever it wants?**

No.

North Carolina law places significant restrictions on law enforcement use of drones for surveillance.

Depending upon the circumstances, surveillance of a person, occupied residence and its curtilage, or private property may require consent, a search warrant, or another recognized legal exception.

The policy specifically requires compliance with these limitations.

### **When may police use a drone without a warrant?**

North Carolina law establishes specific circumstances in which law enforcement drone use may be permitted without a warrant.

Examples can include certain emergencies, pursuit of a suspect, searching for a missing person, circumstances requiring swift action to prevent imminent harm or destruction of evidence, observations that fall within lawful plain-view principles, and certain public gatherings.

Whether a warrant is required depends upon the specific circumstances of the operation.

When legal authority is uncertain and circumstances permit, the policy directs employees to consult a supervisor and, when appropriate, a prosecutor or legal advisor.

### **Who decides when a drone can be deployed?**

Operational deployments should receive supervisory authorization when circumstances permit.

The supervisor considers the purpose of the deployment, legal authority, privacy concerns, whether a warrant or consent may be required, the existence of an emergency, potential risks, and applicable FAA restrictions.

Emergency deployments may occur without prior approval when delay would create an unreasonable risk and the deployment is otherwise lawful. A supervisor must then be notified as soon as reasonably practicable.

### **Who is responsible for safely operating the drone?**

A designated Pilot in Command is responsible for each flight.

The Pilot in Command has final responsibility for determining whether the flight can be safely and legally conducted.

The policy expressly provides that a supervisor may not require a pilot to conduct a flight that the pilot reasonably determines cannot be safely or legally conducted.

### **Are drone pilots required to be trained?**

Yes.

Only authorized and appropriately qualified personnel may operate Department drones.

Pilots must maintain required FAA qualifications and Department proficiency requirements.

Training includes aircraft operation, emergency procedures, FAA regulations, North Carolina law, search-and-seizure requirements, privacy protections, evidence handling, airspace requirements, and operational safety.

## **Does the FAA regulate police drones?**

Yes.

Police Department drones are aircraft and are subject to applicable Federal Aviation Administration requirements.

The policy requires compliance with applicable FAA operating authority, airspace restrictions, aircraft registration, Remote Identification requirements, night-operation rules, restrictions on flying over people or moving vehicles, and other applicable aviation requirements.

## **Is every drone flight recorded?**

Not necessarily.

Recording should occur when it serves a legitimate operational, investigative, evidentiary, training, documentation, or public-safety purpose.

Recordings having evidentiary value are handled through the Department's approved evidence-management procedures.

Employees are prohibited from making personal copies or storing Department drone imagery on unauthorized personal devices.

## **Can drones be used to watch protests, political events, or religious activities?**

The Department may not use drones to monitor lawful First Amendment-protected activity simply because people are exercising those rights.

The policy prohibits surveillance of demonstrations, political activities, religious activities, or similar constitutionally protected activities unless an independent legitimate law enforcement or public-safety purpose exists and the use is otherwise authorized by law.

## **Will the Department use facial recognition or artificial intelligence with its drones?**

Not automatically.

The policy specifically provides that facial recognition, biometric identification, persistent automated tracking, or similar automated

identification technology may not be used merely because a vendor makes that capability available.

Any such capability would require separate legal and operational review, approval by the Chief of Police, and compliance with applicable law and Department policy.

## **SAFEGUARDS AGAINST MISUSE**

The proposed policy contains multiple layers of protection intended to prevent surveillance technology from being misused.

### **Limited Purpose**

Both technologies may only be used for lawful and authorized governmental or law enforcement purposes.

### **Restricted Access**

Only trained and authorized Department personnel may operate the technology or access associated systems and information.

### **Individual Accountability**

Employees use individual credentials, and system activity may be logged and audited.

### **Supervisory Oversight**

Certain searches and drone deployments require or receive supervisory review. More intrusive, prolonged, broad, or sensitive surveillance receives additional scrutiny.

### **Data Retention Limits**

Routine LPR information is subject to the 90-day statutory retention limitation. Drone recordings are retained according to their evidentiary or governmental purpose and applicable records requirements.

## **Restrictions on Information Sharing**

LPR information is confidential, is not a public record under applicable North Carolina law, cannot be sold, and may only be disclosed as permitted by law.

## **Privacy and Constitutional Protections**

The policy expressly prohibits surveillance based solely on protected characteristics and prohibits improper monitoring of lawful First Amendment activities.

## **Audit Requirements**

The Department must audit its ALPR program at least annually and report audit results to the Chief of Police.

## **Documentation**

Historical LPR searches, Department-created alerts, operational drone deployments, legal authority for surveillance, and other significant activities are documented.

## **Vendor Controls**

The policy requires consideration of data ownership, vendor access, cybersecurity, retention, secondary use, information sharing, data breaches, and destruction of Department information.

## **Technology Cannot Expand Its Own Authority**

A particularly important safeguard is that a new capability offered by a technology vendor does not automatically become an authorized police function.

Advanced technologies such as facial recognition, artificial intelligence, biometric identification, predictive analytics, association analysis, or automated tracking must undergo separate legal, privacy, operational, and command review before being used.

## **Complaints and Discipline**

Complaints concerning misuse of surveillance technology are handled through the Department's established complaint and internal investigation process.

Employees who misuse the technology may be subject to disciplinary action and, depending upon the circumstances, civil or criminal liability.

## **OVERALL PURPOSE OF THE POLICY**

The Police Department is not requesting unrestricted authority to conduct surveillance.

The purpose of this policy is to provide officers with modern tools that can improve public safety while placing clear boundaries around how those tools may be used.

The policy is based on four principles:

### **Legitimate Need — Legal Authority — Accountability — Privacy Protection**

The Department's goal is to ensure that surveillance technology remains a focused law enforcement and public-safety tool rather than becoming a means of unrestricted monitoring.

The technology should help the Department locate people in danger, investigate criminal activity, protect officers and citizens, and respond more effectively to emergencies while maintaining appropriate safeguards to protect individual rights and public trust.