WILLIAM & MARY POLICE DEPARTMENT
POLICY AND PROCEDURE

SUBJECT		
LICENSE PLATE READER SYSTEM (LPR)		
P&P SECTION	**P&P NUMBER**	**# OF PAGES**
OPERATIONS	O-35	4
ISSUED BY	**EFFECTIVE DATE**	**REVISED DATE**
Chief Don Butler	07/01/25	12/10/2025
VLEPSC STANDARDS		

I. PURPOSE

The purpose of this policy is to provide William & Mary Police Department (WMPD) personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of LPR information to ensure that the information is used for legitimate law enforcement purposes only and that civil rights and civil liberties of individuals are not violated.

II. POLICY

William & Mary is committed to enhancing the quality of life of the university community by integrating public safety and security best practices with advanced technology. A critical component of a comprehensive security plan is the utilization of a License Plate Reader (LPR) camera system. The LPR network is intended to mitigate known threats, deter crimes, and assist in protecting the personal safety and property of the university community. Due to the large volume of quality images generated by the campus LPR system, WMPD has established protocols to govern the release of any LPR captured images to members of the public.

III. PROCEDURE

A. General Principals

1. The purpose of the LPR network of public areas is to deter crime and to assist the WMPD in maintaining a safe and secure community environment by solving criminal incidents. Any utilization of security technologies and personnel for other purposes would undermine the acceptability of these resources for critical safety goals and is therefore prohibited by this policy.

2. LPR queries in reference to criminal investigations will be conducted in a professional, ethical, and legal manner. Department personnel involved in the use of license plate recognition technology will be properly trained in the responsible use of this technology.

3. The LPR usage will be conducted in a manner consistent with university policy and the Code of Virginia. Enforcement action will not be taken based solely on an LPR alert. Officers must have independent reasonable suspicion or probable cause, or confirmation of other circumstances that confirm the validity of the alert. All LPR system users will receive training prior to using the system. Training may be in-person, virtual, or by written correspondence.

4. The LPR network consists of stationary devices directed at public roadways, which capture images of passing vehicles and their license plates. The LPR network is used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both, into computer-readable data. The LPR system compares the system data to lists of state and federal databases in real time to quickly identify vehicles that have been reported stolen, missing, or suspected of involvement in a crime.

5. WMPD will store LPR system data consistent with the Code of Virginia. Additionally, data will be destroyed automatically within the system, in compliance with the Code. To ensure security of the system, all users must have log-in credentials. Credentials may only be approved by the Chief or Deputy Chief (or designee).

6. If system data is associated with an ongoing criminal investigation, prosecution, or civil action, such data shall be retained until either the investigation concludes without any criminal charges or the final disposition of any criminal or civil matter related to the data, including any direct appeals or writs of habeas corpus pursuant to Code of Virginia 2.2-5517.

7. WMPD prohibits access, use, or dissemination of LPR system data for:

    a. Any purpose that violates the U.S. Constitution or laws of the United States.

    b. Non-law enforcement or personal purposes.

    c. Discriminatory purposes.

    d. Harassing and/or intimidating any individual or group.

e. Targeting of any individual or group by means of camera placement or data use in a discriminatory manner.

f. Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

B. Responsibilities

1. WMPD is solely authorized to select, coordinate, operate, manage and monitor the use of LPR system data for public safety purposes at the university.
2. WMPD will monitor applicable legal developments and security industry practices to ensure that LPR monitoring at the university is consistent with the highest standards and protections.

3. The Deputy Chief (or designee) shall perform an internal audit at least once every 30 days, ensuring use of the LPR system data was consistent with WMPD policy and law. Furthermore, the Deputy Chief (or designee) shall perform a quarterly review of each LPR camera to ensure they are functioning properly. The testing of each camera will include the following:

a. General Functionality

b. Picture Focus

c. Operation during the dark/night hours

d. Operation during the light/day hours

C. Operations

1. The Deputy Chief must ensure that LPR system operators continuously adhere to responsible and proper camera monitoring practices. This will be accomplished by internal audits at least once every 30 days of operator queries and hot list entries to ensure they are consistent with WMPD policy and law.

2. LPRs will only be installed, operated, and used in areas where there is no reasonable expectation of privacy and are in plain view of individuals situated in a public area that is visible to the public.

3. LPR system operators will be trained in the parameters of appropriate LPR use and must acknowledge that they have read and understood the contents of this policy.

D. Dissemination of Images and Information

1. Information obtained from the LPR system is to be used solely for law enforcement in relation to ongoing criminal investigations. LPR system data must be handled with the appropriate level of security to protect against unauthorized access, alteration, or unauthorized disclosure.

2. All appropriate measures will be taken to protect an individual's right to privacy and hold information securely through its creation, storage, transmission, use and deletion. System data will be purged in accordance with the Code of Virginia.

3. The Deputy Chief (or designee) will share LPR system data with other law enforcement agencies in a manner consistent with WMPD policy and the law.
4. The Deputy Chief will confer with the Chief, the Commonwealth Attorney's Office, or the Office of University Counsel, as needed to maintain compliance with the law and WMPD policy in all actions related to the LPR system and system data.