DUBLIN POLICE DEPARTMENT

**STANDARD OPERATING PROCEDURE**

**SECTION: C-006 AUTOMATIC LICENSE PLATE**

**RECOGNITION (LPR) DEVICES**

**EFFECTIVE DATE: 01 JUNE 2021 NUMBER OF PAGES: 3**

**REVISED DATE: DISTRIBUTION AUTHORIZATION:**

#### STANDARD COVERED *CHIEF KEITH MOON*

**N/A**

The purpose of this order is to establish requirements for the use of automatic License Plate Recognition (LPR) devices and access to LPR data.

1. **POLICY**

LPR devices and information contained within LPR databases will be utilized for law enforcement purposes only.

1. **USE**
2. Personnel will exercise due care and caution when utilizing the LPR system and operating a vehicle.
3. Personnel will ensure they are logged into the LPR system under the username assigned to them.
4. An officer may not detain an individual based on an alert from the LPR system unless the officer has reasonable suspicion that such person is involved in criminal activity. Each incident should be weighed according to the totality of circumstances presented therein. The following are general guidelines only but should assist an officer in determining when reasonable suspicion exists concerning various types of LPR alerts.
5. The officer will visually verify that the scanned plate matches the alert information with regard to plate letters, numbers, and the issuing state.
6. Once the state and all characters of the tag have been verified as accurate, the following information should be utilized by an officer in determining whether or not reasonable suspicion exists:
   1. Expired Tags, Insurance, and Other Suspensions – Officers should verify the status of the tag on GCIC to establish reasonable suspicion.
   2. Stolen Vehicles and Stolen License Plates–An alert alone isgenerally sufficient to establish reasonable suspicion.
   3. Wanted Person – A wanted person alert may be utilized as reasonable suspicion unless the officer has information that the wanted subject is not inside the vehicle.
   4. BOLO Only – This alert is information only for officers, and reasonable suspicion may or may not exist based on the alert alone. The narrative of the alert will assist officers in determining the level of reasonable suspicion. Independent reasonable suspicion may or may not be required in order to detain.
   5. CPIC Data – These alerts contain information from the Canadian Police Information Centre. These alerts vary widely and should be read to determine the existence of reasonable suspicion.
   6. Officer Safety, Suspected Gang Member, Sexual Offender, Past Offender, Associate Only, and Information Only –Thesealerts are information only for officers. Reasonable suspicion should be obtained in order to detain.
7. In order to enter a tag into the Local Hotlist (a database containing Dublin Police alerts), an officer should have reasonable suspicion to believe the car is directly associated with the person sought (owner, regular driver, regular passenger, driver or passenger involved in previous criminal activity in said vehicle, etc.), officer information alert, or criminal activity.
8. Once the officer has sufficient evidence based on the above, an entry into the local hotlist may be made through the Dublin Police GCIC/NCIC operator utilizing the Department LPR Entry/Removal Request Form. If a tag has been or will be, entered into GCIC/NCIC or the Department of Revenue hotlist, it should generally not be entered into the Local Hotlist.
9. Only complete tag numbers will be entered into the system. Requests to enter partial tags will be rejected.
10. Officers requesting entry should be cognizant that alerts expire 30 days after entry. Should the officer require renewal of the entry, such renewal may be made through the Dublin Police GCIC/NCIC operator utilizing the Department LPR Entry/Removal Request Form.
11. Once the entering officer is made aware that the alert is no longer valid, he should immediately request the tag to be removed from the system. Removal may be made through the Dublin Police GCIC/NCIC operator utilizing the Department LPR Entry/Removal Request Form.

1. **DATA SECURITY AND ACCESS**

LPR devices/databases will be utilized/accessed for law enforcement purposes only.

Personnel who are granted access to LPR devices and/or databases will be issued a username and password specific to each individual.

When conducting investigative queries into the LPR system, case number (if available), and reason will be entered associated with the search. Queries regarding administrative or auditing purposes will be excluded from the requirement to provide a case number. All investigative queries should only be made through the Dublin Police Network.

Personnel will not release any information obtained by the LPR devices to non-law enforcement personnel unless required by law.

Sample audits will be conducted at least annually to ensure compliance with these requirements. The LPR System Administrator or his designee will be responsible for the audit and retention of audit records.

**IV.** **OPERATOR TRAINING**

Prior to using the LPR system, officers will complete the department-approved training and demonstrate proficiency based on the manufacturer’s recommendations.

1. **DATA STORAGE, RETENTION, AND SHARING**
   * + - 1. The database retention period for all data collected will be 30 days or as required by state or federal law.
   1. Sharing of data will be at the discretion of the Chief of Police or his designee with approval of the Director of Public Safety