BLOOMINGTON POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

AUTOMATIC LICENSE PLATE READERS (ALPR)

Reviewed by:	Jack McQueen	Effective Date:	March 3, 2022
Authorized by:	Chief Jamal Simington	Revision Date:	March 7, 2024

PURPOSE

It is the purpose of this policy to provide Bloomington Police Department personnel with guidelines and principles for the use, collection, access, dissemination, retention and purging of Automatic License Plate Reader (ALPR) data. This policy will ensure that the information is used for legitimate law enforcement purposes only and the privacy, civil rights and civil liberties of individuals are not violated.

This policy assists the Bloomington Police Department in increasing public safety by providing a mechanism to assist in minimizing threats and risk of harm to residents and their property. Proper use of the ALPR system will increase Departmental efficiencies through real time response capability in crimes ranging from potential child abductions to all manners of violent crime. The use of the ALPR system will also assist in post-incident investigations.

DEFINITIONS

Automated License Plate Reader (ALPR)	Any device that automatically scans the license plates of vehicles and using machine learning interprets the alphanumeric values on the plate.
Automated License Plate Reader System	A system that includes ALPR hardware and software that processes license plate images in full or in partial to index scanned license plates into a data system for searching and retrieval.
Law Enforcement Purposes:	The investigation and detection of a crime or violation of law, excluding minor traffic enforcement. Examples include the searches for missing persons or vehicles involved in criminal activity.

POLICY

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

B. Use of the ALPR system, barring exigent circumstances, shall be limited to the investigation of felony-level crimes, crimes against persons, hit and run motor vehicle accidents, persons with active arrest warrants and missing persons.

C. Use of the ALPR system for enforcement of city ordinances, towing, or immigration enforcement is prohibited.

D. The administration, maintenance and training coordination for the ALPR system is the responsibility the Chief of Police or their designee.

E. Ground-based ALPR installation locations will be determined by CIAU through multi-point crime analysis of current criminal incidents, historical criminal incidents, high-density violent crime areas and intersections with a high number of crashes. The recommendation of ALPR installation locations must be approved by the Chief of Police or their designee. Existing ALPR installations may only be relocated after receiving approval by the Chief of Police or their designee after following a similar analysis of criminal incidents near the proposed installation location. Additionally, each BPD patrol vehicle is equipped with onboard ALPR technology and this capability is automatically enabled when a patrol vehicle is powered on, and the mobile data computer is on-line. The in-car ALPR system shall be used on a daily basis.

F. An officer may not detain an individual based on the alert from the ALPR system unless the officer has reasonable suspicion that such person is involved in criminal activity.

G. Officers will verify all ALPR alerts prior to taking enforcement action. Verification should include the visual inspection of the scanned license plate image, license plate letters/numbers, the issuing state as well as an examination of the vehicle image. The officer should also verify the plate match of the vehicle in question by also comparing the vehicle make, model and any other descriptors provided in the ALPR alert. Verification may also be assisted through use of a query on the vehicle registration via the Illinois Law Enforcement Data System Agencies (LEADS) and NCIC.

H. Creation and use of internal BPD Custom Hot List for investigation

   a. BPD's internal Custom Hot List is considered confidential information to the extent permitted by law.

   b. Use and creation of BPD's internal Custom Hot List is limited to members of the Criminal Investigations Division and BPD detectives assigned to ISP Task Force 6.

   c. BPD's Custom Hot List is a list of vehicle registrations in which detectives have reasonable suspicion to believe the vehicle is legitimately associated with the commission of a criminal offense or involved in or planning criminal conduct or activity that presents a danger to any individual or community, or the person sought.

   d. Once a detective has sufficient evidence based on the above, an entry into the BPD internal Custom Hot List may be made only after being approved by the Criminal Investigations or Street Crimes Division Lieutenant.

   e. Entries into BPD's internal Custom Hot List must be a complete license plate. Partial plate entries are prohibited.

   f. Detectives creating an entry into the BPD internal Custom Hot List shall set the entry to expire in no longer than 30 days from the date of entry. Detectives wishing to extend an entry past 30 days shall extend the entry for another 30 days with approval of a Criminal Investigations or Street Crimes Lieutenant. Commanders creating an entry into the BPD Custom Hot List are responsible for the removal of their list by the end of their shift or they shall coordinate with the oncoming shift commander to continue the use of the list on the

next shift. If use of the Custom Hot List is continued to the next shift, the oncoming shift commander shall take responsibility for removal of the list at the end or their shift.

g. Once the entering commander/detective is made aware that their ALPR alert is no longer valid, they should remove the vehicle from the BPD internal Custom Hot List or request or have it removed by the ALPR system administrator as soon as possible.

h. Custom Hot Lists shall not be created for investigations involving crimes in other jurisdictions unless the BPD Hot List creator is working a joint investigation with the outside agency(s).

I. If officer(s) are following a stolen vehicle that has alerted on the BPD ALPR system, and that vehicle enters Normal prior to enforcement action, officers shall notify Normal Police Department that they have entered Normal's jurisdiction prior to any enforcement action(s).

DATA SECURITY, ACCESS, AND PRIVACY

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

A. The Bloomington Police Department will not utilize the ALPR system to seek data on any individual or organization based solely on their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, age, disability, gender, gender identity, sexual orientation or other classification protected by law.

B. Employees shall not use the ALPR system to target any group or individual in a discriminatory manner or infringe on constitutionally protected activities. This shall not preclude the Chief of Police or the system administrator from releasing general information as to the effectiveness of the ALPR program and other such communications.

C. Access to the ALPR system for the purpose of queries will be granted to all BPD supervisors, officers, dispatchers, and criminal analysts. Normally, the use of the ALPR system for queries must be related to missing persons, criminal investigations, or administrative system testing. All users that are granted access to ALPR system will be issued a unique username and password. The use of another employee's username and password is prohibited. The sharing of an employee's username and password is also prohibited. Employees that are terminated from employment or no longer need access to the ALPR system will promptly have their access rights removed.

D. The use of ALPR systems is further restricted in the following ways:

1. Dispatcher user accounts will limit their searches to the local BPD and NPD ALPR network of cameras.

2. Police Officer user accounts will enable search capability across the BPD ALPR network and other agency networks from law enforcement agencies that have agreed to ALPR data sharing.

3. Detectives and Criminal Analyst's user accounts will match those of police officers with the addition of creation and use of BPD Custom Internal Hot Lists.

E. When conducting investigative queries into an ALPR database, the requestor is required to enter either a case number (when available), a CAD run number, or a descriptive term/phrase describing their search when a case or run number have yet to be established. Descriptive phrase examples are "Stolen Vehicle", "Shots Fired", "Suicidal Subject", etc. This entry will be placed in the "Search Reason" or "Lookup Reason" fields in the ALPR interface. Doing so associates a user search with a reason for the search in the system audit logs. Queries for administrative or auditing purposes will be excluded from the requirement to provide a case number.

F. Employees are prohibited from releasing any information obtained from the ALPR system to any non-law enforcement personnel unless required by law or specifically authorized by this policy. Personnel accessing the ALPR data shall also follow BPD SOP 5.26, Protected Information, which controls the access, transmission, release, and security of protected information.

G. The ALPR phone application shall only be installed and used on departmentally issued work phones. Use of the ALPR phone application is limited to Sworn Officers and members of the Crime and Intelligence Analysis Unit. The ALPR phone application shall not be paired with any personally owned device. When off-duty, officers shall select the off-shift mode on the ALPR phone application to avoid receiving live system alerts.

DATA STORAGE, RETENTION and SHARING

A. The database retention period for all data collected by BPD ALPR hardware and stored on the ALPR cloud storage system shall not exceed 30 days. Mass downloading (data dumps or mass data exports) of ALPR data via the ALPR cloud storage system is prohibited.

B. Collected ALPR data is encrypted and held in an AWS CJIS compliant cloud. Because this cloud is vendor owned, data contained in the ALPR cloud is not subject to request or disclosure under the Illinois Freedom of Information Act. Individual ALPR data records downloaded as part of an active investigation become records of the Department. Individual ALPR records that are downloaded for use in an investigation are subject to Illinois FOIA request like all other data and records belonging to the Department. Downloaded records are to be treated as evidence and stored according to Departmental procedures and policy by the ALPR end user. Evidence created through use of ALPR query shall also be included in an officer's/analyst's investigative report and uploaded to Evidence.com as directed in Policy 3.05 "Management of Digital Exhibits in Evidence.com".

C. External law enforcement agencies may request individual queries of the Department's ALPR system as part of an active criminal investigation by the external law enforcement agency. The Department will only share BPD ALPR data for official law enforcement purposes in accordance with Departmental policies and local, state, and federal laws and regulations. If the external agency request produces investigative leads in other jurisdictions, BPD will not provide records from those external agencies to the requesting agency. BPD will then refer the requesting agency to the outside agency where the original records reside.

    a. When practical, and in absence of exigent circumstances, external law enforcement requests should be referred to CID Command or members of CIAU for processing and record keeping.

D. BPD ALPR data shall not be shared with any commercial, contracted, or private entity.

E. Electronic online sharing of historical Departmental ALPR data to external law enforcement agencies, who use a compatible ALPR system, is permissible and will be at the discretion of the Chief of Police or their designee. Electronic online sharing of historical Departmental ALPR data shall be limited to state and local law enforcement agencies within the state of Illinois. As directed in 625 ILCS 5/2-130, the Department will not share any ALPR data with out-of-state agencies for the purpose of investigating or enforcing a law that denies or interferes with a person's right to choose or obtain reproductive health care services or any lawful health care services as defined by the Lawful Health Care Activity Act; or permits the detention or investigation of a person based on the person's immigration status.

F. Absent exigent circumstances, electronic online sharing of historical Departmental ALPR data to federal law enforcement agencies is prohibited. This prohibition does not preclude a federal agency from requesting an individual ALPR record query as explained above in point C.

G. At no time is ALPR data allowed to be sold, monetized, or otherwise used for any commercial or non-law enforcement purpose.

TRAINING

The Department will establish end-user training for those employees provided direct access to ALPR data. ALPR system users shall be trained prior to being granted access to the ALPR system(s). Training will include a review of this policy and Policy 5.26 "Protected Information", the proper handling/storage of ALPR downloaded records, searching of the ALPR system(s), the requirements and process of creating and deleting entries into the BPD internal Hot List, guidance regarding the appropriate uses of ALPR technology and possible penalties for ALPR policy violations.

ACCOUNTABILITY

A. Agency user audit reports will be produced and inspected monthly to ensure compliance with this policy. The system administrator will be responsible for conducting the monthly audit and reporting any discrepancies, problems or misuse to the Chief of Police or their designee. The monthly user audit will also contain anonymized user data and transactional data suitable for release on the Department's web-based Transparency Portal.

B. Agency user audit reports will be produced monthly. Updates regarding the BPD ALPR program will be presented at the monthly Public Safety Community Relations Board (PSCRB) meetings. These updates will provide the basis for ongoing discussions with PSCRB as it pertains to the department's use of ALPR technology.

C. Any Department member found to be in noncompliance with this policy regarding their use of the ALPR system will immediately have their access suspended to the ALPR system (if an authorized user) and may be subject to the appropriate disciplinary or administrative actions.

D. Any non-Departmental personnel found to have gained unauthorized access will be referred to the appropriate authorities for criminal prosecution, as necessary.