

Resolution No. 28-26

A RESOLUTION OF THE BOROUGH OF MERCERSBURG, FRANKLIN COUNTY, PENNSYLVANIA, ESTABLISHING AN OPERATIONAL POLICY, DATA RETENTION STANDARDS, AND OVERSIGHT PROTOCOL FOR AUTOMATED LICENSE PLATE READER (ALPR) SYSTEMS, INCLUDING FLOCK SAFETY CAMERAS.

WITNESSETH

WHEREAS, the Borough Council of the Borough of Mercersburg recognizes that Automated License Plate Reader (ALPR) systems—including Flock Safety cameras—provide advanced technology that enhances public safety, assists in criminal investigations, and secures municipal borders; and

WHEREAS, the physical Flock Safety camera hardware, implementation infrastructure, and associated operational fees have been generously provided to the Borough as a 100% community donation received from the Mercersburg Moose Lodge; and

WHEREAS, Section 1202 of the Pennsylvania Borough Code (8 Pa.C.S. § 1202) grants the Borough Council the corporate power to look after the safety, health, and welfare of the citizens of the Borough, as well as the authority to accept and manage donations of property and funds for public purposes; and

WHEREAS, the Pennsylvania Title 75 (Vehicle Code) and established law enforcement guidelines permit the utilization of technology for the detection of stolen vehicles and wanted persons, provided that public privacy and constitutional protections are rigidly safeguarded; and

WHEREAS, the Pennsylvania Right-to-Know Law (65 P.S. § 67.101 et seq.) establishes statutory guidelines for the public accessibility, exemptions, and redaction protocols of records held by local government agencies.

NOW, THEREFORE, BE IT RESOLVED, that the Borough Council of the Borough of Mercersburg hereby adopts the following Automated License Plate Reader (ALPR) Operational and Data Policy:

SECTION 1: Purpose & Scope

- **Scope:** This policy applies to all Automated License Plate Reader (ALPR) systems, hardware, software, data capture mechanisms, and cloud-hosted data infrastructure (including Flock Safety networks) owned, operated, leased, or accessed by the Borough of Mercersburg and its law enforcement personnel.
- **Purpose:** The sole intent of this technology is to enhance public safety through efficient data collection used exclusively for legitimate law enforcement actions.

SECTION 2: Authorized Law Enforcement Use

In strict accordance with municipal public safety mandates, ALPR systems shall be used solely based on a documented law enforcement purpose, including:

- **Criminal Investigations:** The active investigation of criminal activity, fleeing suspects, and identifying vehicles tied to active cases.
- **Asset Recovery:** The identification and recovery of stolen vehicles or stolen license plates.
- **Life Safety Operations:** The location of wanted individuals, missing persons, or individuals subject to an AMBER Alert or Silver Alert.
- **Threat Mitigation:** Active responses to specific, articulable, and immediate threats to public safety or critical infrastructure.

SECTION 3: Prohibited Operational Practices

To ensure compliance with constitutional protections and civil liberties, the following uses of ALPR systems are strictly prohibited:

- **Indiscriminate Surveillance:** Systems shall not be used for general, random, or arbitrary tracking of individuals or vehicles without legal justification.
- **Protected Activities:** System data shall not be used to monitor or track individuals engaging in constitutionally protected activities (e.g., political rallies, religious services, peaceful assemblies) absent an active, independent criminal investigation.
- **Immigration Enforcement:** Systems shall not be utilized for civil immigration enforcement actions unless explicitly mandated by federal or state law.
- **Generalized Databases:** The Borough shall not create, expand, or maintain generalized databases of localized vehicle movements that are unrelated to a specific, active investigation.

SECTION 4: Data Retention & Safeguards

- **Standard Retention:** All captured ALPR data, images, and meta-logs shall be automatically purged and permanently deleted after a maximum period of Thirty (30) days from the time of capture.
- **Retention Extensions:** Data may be preserved beyond thirty (30) days only if it is explicitly logically linked to:
 - An active, open criminal investigation.
 - A valid, legally executed court order or subpoena.
 - A reasonably anticipated civil or criminal claim involving the Borough.
- **Documentation:** Any extended data retention must be documented with a clear case-specific justification filed within the department.

SECTION 5: Access Controls & Security Infrastructure

- **Personnel Restrictions:** Access to the ALPR system platform, search fields, and historical logs is strictly limited to law enforcement personnel who have undergone formal training on the system.
- **Search Justification:** System users are prohibited from executing random or exploratory searches. Each login and data query requires a documented, case-specific justification (such as an incident number or active case file reference).
- **Audit Logging:** The platform must attach an unalterable, system-generated audit trail—including user IDs, precise timestamps, and specific query terms—for every single login and data search performed.

SECTION 6: Inter-Agency Data Sharing & Commercial Prohibitions

- **Authorized Law Enforcement Sharing:** ALPR data may be shared with or transferred to outside law enforcement and public safety agencies only for legitimate, verified investigative purposes or as explicitly required by state or federal law.
- **Transfer Logging:** All data-sharing transmissions, electronic transfers, or cross-agency network connections must be permanently logged in the audit trail.
- **Commercial Prohibition:** Under no circumstances shall the Borough sell, lease, or share ALPR data, metadata, or images with private entities, commercial vendors, or non-law-enforcement third parties.

SECTION 7: Right-to-Know Compliance & Redaction Protocols

- **Statutory Review:** Public requests for ALPR records submitted under the Pennsylvania Right-to-Know Law shall be strictly evaluated by the Open Records Officer in accordance with applicable statutory exemptions, specifically focusing on criminal investigation and public safety exemptions.
- **Bulk Request Denial:** To protect individual privacy rights, all bulk or generalized data requests for non-specific vehicle lists or timeline history shall be denied to the maximum extent permitted by law.
- **Redaction Mandate:** Where partial access to a record is legally required, strict redaction processes must be utilized to mask unrelated license plates, sensitive personal data, or uninvolved vehicles before release.

SECTION 8: Audit, Oversight, and Vendor Accountability

- **Independent Audits:** Internal control reviews and periodic audits of the system's transaction history, search logs, and retention timelines shall be conducted regularly to verify compliance with this policy.
- **Disciplinary Action:** Any unauthorized access, misuse of data, or willful violation of these regulations by an employee shall result in immediate revocation of access privileges

and severe disciplinary action, up to and including termination and criminal prosecution where applicable.

- **Vendor Requirements:** Any third-party technology vendor (including Flock Safety) contracted by the Borough must agree in writing to:
 - Maintain strict alignment with all aspects of this policy.
 - Impose robust, industry-standard data security safeguards and encryption protocols.
 - Never retain, harvest, or sell the Borough's operational data for proprietary or commercial use.

DULY ADOPTED AND RESOLVED this 13th day of July, 2026, by the Borough Council of the Borough of Mercersburg in lawful session duly assembled.

BOROUGH OF MERCERSBURG:

By: Kelvin Craig

Borough Council President

APPROVED BY THE MAYOR:

By: [Signature]

Mayor

ATTEST:

By: [Signature] [Signature]

Borough Manager/Secretary (SEAL)

