Automated License Plate Readers (ALPRs)

426.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

426.2 POLICY

The policy of the Ayer Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

426.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Ayer Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Deputy Chief. The Deputy Chief will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

426.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official law enforcement purposes by authorized personnel.

(b) Authorized access to an ALPR may be used in conjunction with an investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) No authorized member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(d) No ALPR operator may access confidential department, commonwealth, or federal data unless authorized to do so.

(e) If practicable, the officer should verify an ALPR response through the appropriate official law enforcement database before taking enforcement action that is based solely on an ALPR alert.

426.5 DATA COLLECTION AND RETENTION

The Deputy Chief is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be stored and retained in accordance with department procedures.

All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data should be downloaded onto portable media and booked into evidence.

426.6 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The Ayer Police Department will observe the following safeguards regarding access to and use of stored data:

(a) All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

(b) Members authorized to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

426.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The Massachusetts agency makes a request through the network interface for the ALPR data.

(b) The non-Massachusetts agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(c) The request is reviewed by the Deputy Chief or the authorized designee and approved before the request is fulfilled.

(d) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Public Safety Video Surveillance System

336.1 PURPOSE AND SCOPE

This policy provides guidance for the placement and monitoring of department public safety video surveillance, as well as the storage and release of the captured images.

This policy only applies to overt, marked public safety video surveillance systems operated by the Department. It does not apply to mobile audio/video systems, covert audio/video systems, or any other image-capturing devices used by the Department.

336.2 POLICY

The Ayer Police Department operates a public safety video surveillance system to complement its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance public safety and security in public areas. Cameras may be placed in strategic locations throughout the Town to detect and deter crime, to help safeguard against potential threats to the public, to help manage emergency response situations during natural and man-made disasters, and to assist Town officials in providing services to the community.

Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

336.3 OPERATIONAL GUIDELINES

Only department-approved video surveillance equipment shall be utilized. Members authorized to monitor video surveillance equipment should only monitor public areas and public activities where no reasonable expectation of privacy exists. The Chief of Police or the authorized designee shall approve all proposed locations for the use of video surveillance technology and should consult with and be guided by legal counsel as necessary in making such determinations.

336.3.1 PLACEMENT AND MONITORING

Camera placement will be guided by the underlying purpose or strategy associated with the overall video surveillance plan. As appropriate, the Chief of Police should confer with other affected Town divisions and designated community groups when evaluating camera placement. Environmental factors, including lighting, location of buildings, presence of vegetation, or other obstructions, should also be evaluated when determining placement.

Cameras shall only record video images and not sound. Recorded images may be used for a variety of purposes, including criminal investigations and monitoring of activity around high-value or high-threat areas. The public safety video surveillance system may be useful for the following purposes:

(a) To prevent, deter, and identify criminal activity.

(b) To target identified areas of gang and narcotics complaints or activity.

(c) To respond to critical incidents.

(d) To assist in identifying, apprehending, and prosecuting offenders.

(e) To document officer and offender conduct during interactions to safeguard the rights of the public and officers.

(f) To augment resources in a cost-effective manner.

(g) To monitor pedestrian and vehicle traffic activity.

Images from each camera should be recorded in a manner consistent with the underlying purpose of the particular camera. Images should be transmitted to monitors installed in the Shift Supervisor's office and Central Communications. When activity warranting further investigation is reported or detected at any camera location, the available information should be provided to responding officers in a timely manner. The Shift Supervisor or trained Central Communications personnel are authorized to adjust the cameras to more effectively view a particular area for any legitimate public safety purpose.

The Chief of Police may authorize video feeds from the public safety video surveillance system to be forwarded to a specified location for monitoring by other than police personnel, such as allied government agencies, road or traffic crews, or fire or emergency operations personnel.

Unauthorized recording, viewing, reproduction, dissemination, or retention of anything documented by public safety surveillance equipment is prohibited.

336.3.2 INTEGRATION WITH OTHER TECHNOLOGY

The Department may elect to integrate its public safety video surveillance system with other technology to enhance available information. Systems such as gunshot detection, incident mapping, crime analysis, license plate recognition, and other video-based analytical systems may be considered based upon availability and the nature of department strategy.

The Department should evaluate the availability and propriety of networking or otherwise collaborating with appropriate private sector entities and should evaluate whether the use of certain camera systems, such as pan-tilt-zoom systems, video enhancement, or other analytical technology, requires additional safeguards.

336.4 VIDEO SUPERVISION

The Deputy Chief should monitor video surveillance access and usage to ensure members follow department policy and applicable laws. The Deputy Chief should ensure such use and access is appropriately documented.

336.4.1 VIDEO LOG

A log should be maintained at all locations where video surveillance monitors are located. The log should be used to document all persons not assigned to the monitoring locations who have been given access to view or monitor images provided by the video surveillance cameras. The logs should, at a minimum, record the:

(a) Date and time access was given.

(b) Name and agency of the person being given access to the images.

(c) Name of person authorizing access.

(d) Identifiable portion of images viewed.

336.4.2 PROHIBITED ACTIVITY

All video surveillance will be closely safeguarded and protected by both procedural and technological means. The Ayer Police Department will observe the following safeguards regarding access to and use of stored data:

(a) All video surveillance shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

(b) Members authorized to access video surveillance under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) Video surveillance system audits should be conducted on a regular basis.

Video surveillance equipment shall not be used to harass, intimidate, or discriminate against any individual or group.

336.5 STORAGE AND RETENTION OF MEDIA

All downloaded media shall be stored in a secure area with access restricted to authorized persons. A recording needed as evidence shall be copied to a suitable medium and booked into evidence in accordance with established evidence procedures. All actions taken with respect to retention of media shall be appropriately documented.

The type of video surveillance technology employed and the manner in which recordings are used and stored will affect retention periods. The recordings should be stored and retained in accordance with the established records retention schedule.

336.5.1 EVIDENTIARY INTEGRITY

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates, and date and time stamping shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

336.6 RELEASE OF VIDEO IMAGES

All recorded video images gathered by the public safety video surveillance equipment are for the official use of the Ayer Police Department.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records.

Requests for recorded images from other law enforcement agencies shall be referred to the Shift Supervisor for release in accordance with a specific and legitimate law enforcement purpose.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

336.7 VIDEO SURVEILLANCE AUDIT

The Chief of Police or the authorized designee will conduct an annual review of the public safety video surveillance system. The review should include an analysis of the cost, benefit, and effectiveness of the system, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline, or policy.

The results of each review shall be appropriately documented and maintained by the Chief of Police or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy should be promptly addressed.

336.8 TRAINING

All department members authorized to operate or access public safety video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, interaction with dispatch and patrol operations, and a review regarding relevant policies and procedures, including this policy. Training should also address commonwealth and federal law related to the use of video surveillance equipment and privacy.