



# Alexandria Police Department



## Directive 2.9

### Public Safety Cameras

Effective Date: 06-01-2024

Cancels: This is a new directive.

Updated Date:

Section(s):

SME Review Date: 2027

Updated Date:

Section(s):

Updated Date:

Section(s):

#### CONTENTS

- 2.9.01 PURPOSE/POLICY
- 2.9.02 DEFINITIONS
- 2.9.03 PLACEMENT OF PUBLIC SAFETY CAMERAS
- 2.9.04 STORAGE AND ACCESS
- 2.9.05 PROHIBITED USES
- 2.9.06 PROVISIONS OF PUBLIC SAFETY CAMERA FILES
- 2.9.07 SUPERVISOR RESPONSIBILITIES

#### 2.9.01 PURPOSE/POLICY

1. The purpose of the Public Safety Camera (PSCs) policy is to define the manner in which Public Safety Cameras will be used to support the City of Alexandria Police Department's (APD) public safety mission. This policy applies to all Department personnel that use PSC's.
2. The City of Alexandria Police Department employs Public Safety Cameras to proactively deter crime, bolster public safety efforts, and to provide valuable assistance in investigations.
3. The operation of PSCs in public spaces does not require a warrant or court order, allowing for the monitoring of public spaces.
4. The City of Alexandria Police Department highly prioritizes safeguarding the privacy, civil rights, and liberties of the community members within the City of Alexandria. This policy safeguards individual's privacy rights in accordance with the City of Alexandria's core values while also following all Federal, State and City of Alexandria laws, codes, and regulations. It formalizes procedures and the authority of the City of Alexandria Police Department to handle, view, retain, disseminate, and the destruction of video footage.
5. This policy does not imply or guarantee that PSCs will be monitored.

6. This policy does not supersede and does not apply to the use of covert cameras utilized to further covert operations.

### 2.9.02 DEFINITIONS

1. Cloud-Based Storage: a virtual computer storage system, to which documents, photographs, videos, and other forms of media are stored on a virtual or cloud server hosted by a third party.
2. Edge Storage: A device designed to collect and store electronic data on a recording device, using a solid-state drive (SSD) or other locally installed drive.
3. Electronic File Management System (EFMS): A system consisting of recording devices (ICC, BWC, LPR, PSC, etc.) and a cloud-based storage system which houses digital evidence captured by these systems, as well as digital evidence gathered by sources outside the system. For the purposes of this directive, this solely refers to Evidence.com as our current EFMS.
4. PSC Digital Evidence File: A recording of video evidence captured from a PSC device.
5. Public Safety Camera (PSC): A mounted video recording device which has been constructed by City of Alexandria employees or vendors for the purposes of capturing video within public areas.
6. Video Management System (VMS): A software-based platform that is used to manage and control video surveillance cameras, recording devices, and other security components.

### 2.9.03 PLACEMENT OF PUBLIC SAFETY CAMERAS

1. Consideration for placement of PSCs will be determined by a variety of factors, to include, but not limited to, the following:
  - a. Areas with acute criminal activity.
  - b. Areas with a documented history of criminal activity.
  - c. Areas where the placement of a PSC would be beneficial in crime reduction strategies.
  - d. City sponsored events.
  - e. City sponsored initiatives.
  - f. Any other location to further the mission of the Alexandria Police Department.
2. Requests for placement of PSCs should be made in writing to the Technology Services Division. The request should include the area to be observed, the type of camera requested, the time frame to which the camera is needed, and the supporting crime statistics and/or relevant justification.

3. The Technology Services Division will make every effort to accommodate the request; however, it has the authority to place, move, or remove a PSC for higher priority needs.

## **2.9.04 STORAGE AND ACCESS**

### **A. STORAGE**

1. All PSC digital evidence files shall be securely stored in accordance with the Virginia Public Records Act and the retention schedules for law enforcement records issued by the Library of Virginia.
2. PSC digital evidence files that do not have administrative or evidentiary value will be retained in accordance with General Schedule (GS) 17 Records Retention guidelines for law enforcement records, for a minimum of seven (7) days after the recorded event.
3. PSC digital evidence files that have administrative or evidentiary value will be retained in accordance with the Virginia General Schedule (GS) 17 Records Retention guidelines for law enforcement records. Upon identification of a file that has evidentiary value, the file shall be retained by transferring the file into the Departments Electronic File Management System (EFMS), and utilizing procedures outlined in police directive 2.8 Body-Worn Cameras placed into one of three categories for retention, as follows:
  - a. Category 2: Formal Contacts with No Criminal Activity: This category pertains to BWC activations during law enforcement interactions, including but not limited to traffic stops, subject checks, and service calls that do not involve any actual or suspected criminal activity. Records are retained according to appropriate schedules, such as Series 200148, with a minimum retention period of five years.
  - b. Category 3: Formal Contacts Involving Actual or Suspected Misdemeanor Crimes: This category includes any recording related to an official law enforcement contact involving an actual or potential misdemeanor offense. Records are retained according to appropriate schedules, such as Series 200147, with a minimum retention period of fifty years.
  - c. Category 4: Formal Contacts Involving Actual or Suspected Felony Crimes: This category includes any recording related to an official law enforcement contact involving an actual or potential felony offense. Records are retained according to appropriate schedules, such as Series 200145, with a minimum retention period of one hundred years.
4. APD shall preserve all digital evidence files related to any criminal proceeding, claim filed, pending litigation, or administrative investigation until the matter is resolved or as required by applicable laws, whichever is greater.
5. Categories and retention periods for recorded files may change if the Library of Virginia updates the retention schedules. All retained recordings will be assigned a retention category, and after the retention period is over, the recordings will be expunged from the

Department's system in accordance with the record destruction procedures established by the Library of Virginia.

6. All PSC digital evidence files are stored locally utilizing Edge Storage devices, located on the device as well as within a cloud-based storage system for a minimum of 7-days.

## **B. ACCESS**

1. The Alexandria Police Department Technology Services Division has the authority to select, coordinate, operate, manage, and monitor all PSC's pursuant to this policy.
2. All PSC digital evidence files, including images, videos, audio, and data, are the property of the APD. Employees shall not copy, publish, share, release, or disseminate any PSC recordings except to support a bona fide investigation to a law enforcement officer. Authorization by the Chief of Police or the designee acting in the Chief's absence is required to release PSC recordings to anyone other than a law enforcement officer, unless otherwise defined within this policy.
3. Employees shall not edit, delete, or alter any PSC recordings, except as authorized by the Chief of Police, or the designee, unless otherwise defined within this policy.
4. Employees are permitted to view live footage and access historical PSC digital evidence files solely for valid law enforcement purposes only, including but not limited to report writing, court preparation, and investigative activities.
5. When an employee determines that an incident or digital evidence may have been captured by a PSC, and not captured by either a Body-Worn Camera or an In-Car Camera, they shall review the PSC digital file to determine if exculpatory evidence may exist.
6. Public Safety Digital Evidence File Requests
  - a. A Department member requiring assistance with obtaining a copy of a historical Public Safety Camera digital evidence file shall complete a Public Safety Camera Digital Evidence File Request in electronic format and submit it to the Technology Services Division in a timely manner.
  - b. It is the responsibility of the requestor to complete the request prior to the time to which the video has been overwritten [2.09.04.A.2].
  - c. Public Safety Camera requests shall be processed by the Technology Services Division using the information provided by the requestor.
  - d. When extracting live video footage, photographs or other digital evidence data for future use, the files shall be tagged with the call for service number, case number, or employee serial number, within the VMS. The video should then be transferred to evidence.com for retention.

- e. All Public Safety Camera digital evidence file requests shall be documented by electronic means, as determined by the Technology Services Division.
7. The use of electronic analytics shall only be utilized by the Technology Services Division or those trained to operate the analytic software.

#### **2.9.05 PROHIBITED USES**

1. Users of the Public Safety Cameras may use the information collected from PSCs only for legally authorized law enforcement purposes and may not use that information to unlawfully discriminate against people based on race, color, sex or gender, religion, national origin, marital status, age, disability, sexual orientation, or gender identity.
2. All recordings, including images, videos, audio, and data, are the property of the APD. Employees shall not copy, publish, share, release, or disseminate any Public Safety Camera digital evidence file except to support a bona fide investigation, to a law enforcement officer. Authorization by the Chief of Police or the designee acting in the Chief's absence is required to release recordings to anyone other than a law enforcement officer.
3. The Public Safety Camera shall not be used for the purposes of audio voice recordings. If a public safety camera is equipped with audio voice recording technology, it shall not be used, unless authorized by the Chief of Police, or the appointed designee.
4. The Public Safety Camera shall not be used for the purposes of facial recognition, unless authorized by the Chief of Police, or the appointed designee. If authorization is granted, it will be executed as defined in VA Code § 15.2-1723.2.
5. The Public Safety Camera shall not be used for the intended purpose of viewing areas where there is a reasonable expectation of privacy, to include viewing inside a private residence, private structure, concealed curtilage, or other areas subject to the reasonable expectation of privacy, unless explicitly pursuant to a lawful consent, exigent circumstances, signed court order or search warrant.

#### **2.9.06 PROVISIONS OF PUBLIC SAFETY CAMERA FILES**

##### **A. DISCOVERY**

1. The Commonwealth Attorney's Office is primarily responsible for fulfilling discovery requests, but if an employee becomes aware that a video may not have been shared or is unable to locate the requested video, they shall immediately contact the Technology Services Division. The Technology Services Division shall send/re-send the file so that the Commonwealth Attorney's Office can satisfy their discovery obligations.
2. If the Commonwealth Attorney's Office has not entered their appearance, individuals may request access to PSC files through legal means such as Discovery and Virginia FOIA.

## **B. SUBPOENA AND COURT ORDERS**

1. The Technology Services Division will review PSC data when requested by subpoena or court order and will communicate any applicable concerns regarding their release (e.g., sexual assault, juvenile, or gang-related cases) to the Information Services Section Commander, or designee.
2. If the Technology Services Division receives a subpoena or court order related to a pending criminal case from anyone other than the Office of the Commonwealth's Attorney, the Technology Services Division shall notify the prosecutor assigned to the case before complying to determine if any legal action should be taken prior to compliance.

## **C. MUTUAL AID AND SHARING OF PSC FILES**

1. Outside law enforcement agencies may request PSC footage related to criminal investigations. Employees may share PSC files if the request supports a bona fide criminal investigation. If an employee has concerns about releasing the footage, they should communicate this to their supervisor who will provide guidance. Any mutual aid requests related to administrative matters should be brought to the attention of the Office of Professional Responsibility and/or the Technology Services Division for review and approval.

## **D. MEDIA RELEASE**

1. PSC files cannot be released to the media without the prior approval of the City Manager and/or the Chief of Police, or their designee acting in their respective absence. When PSC data is approved for media release, privacy of all parties, criminal investigations, and APD interests shall be protected. Redaction software should be used to blur faces, skin, addresses, license plates, or any sensitive materials that could compromise an investigation or place individuals in danger. When footage is released for identification purposes, only footage that can aid in the effort shall be provided with great care.

## **E. VIRGINIA FREEDOM OF INFORMATION ACT (FOIA)**

1. PSC files may be requested through Virginia FOIA, and the City Attorney's Office will assist in processing FOIA requests. When an investigation or court proceedings are ongoing, the request may be denied if it compromises the criminal justice process or falls under another FOIA exemption. When the Chief of Police or their designee approves the release of PSC footage, it may be appropriately redacted, using software to blur faces, skin, addresses, license plates, or other sensitive materials. Great care shall be taken when releasing PSC data as a result of a FOIA request to avoid compromising investigations, violating citizens' privacy, or affecting APD interests.

## **F. EXPUNGEMENT**

1. The Technology Services Division is responsible for reviewing, processing, and deleting any items subject to an Expungement Order. The review will confirm the number of suspects involved in the case. If the person named in the order is the sole suspect, all

evidentiary items related to that case will be deleted in accordance with the order. If multiple suspects are involved, only the expunged person's identifying information will be redacted from related items, and the redacted version depicting the non-expunged suspects will be retained. Any deleted items will be noted as per court-ordered expungement.

## **G. REDACTION**

1. For the purposes of this directive, redactions will be completed by the Technology Services Division, and the designee(s) shall be appointed by the Technology Services Division Commander.

### **2.9.07 SUPERVISOR RESPONSIBILITIES**

1. The Technology Services Division is responsible for managing and administering the PSC program, including all associated equipment and software.
2. Technology Services Division supervisor's administrative duties include, but is not necessarily limited to, procurement of PSC equipment, construction of PSC equipment, coordinating maintenance and warranty service with the vendor, function checking the system and files, providing technical assistance, coordinating repair and replacement of systems, conducting annual inspections, audits, responding to public records requests and redacting PSC files as required by law, providing statistical and analytical support, file restriction, and forensic review of PSC files, and coordinating with outside departments such as the City Attorney's Office, Commonwealth Attorney's Office, and Information Technology.
3. All supervisors are responsible for ensuring that employees within their command are utilizing PSCs in accordance with this policy and address any deviations expeditiously and in accordance with Department policy.

**BY AUTHORITY OF:**

**Raul Pedroso**  
**Interim Chief of Police**