





POLICIES AND PROCEDURES MANUAL

	PUBLIC SAFETY SURVEILLANCE CAMERAS	
	POLICY NUMBER: 41-13	ISSUING AUTHORITY 
	EFFECTIVE DATE: June 24, 2025	Christine A. Elow Police Commissioner

I. GENERAL CONSIDERATIONS AND GUIDELINES

Public Safety surveillance cameras may be permanently deployed by the City of Cambridge in areas with public access to assist the Police Department in providing for public safety and investigations. These cameras do not record audio, have no search function, cannot create a searchable record of license plate data, have no facial recognition technology, and will be recording and capturing video content 24/7 but will not be regularly monitored on a real-time basis unless there is an emergency that requires real-time monitoring. All captured video content will be stored and housed at the Cambridge Police Department for 30 days, unless a request has been made to preserve the footage from a CPD employee, an outside law enforcement agency, or from internal personnel fulfilling a Public Records Request or subpoena.

II. POLICY

It is the policy of the Cambridge Police Department to:

- A. manage and control the use of the system to assist in providing for public safety and security;
- B. comply with all applicable CJIS and CORI rules, regulations, and policies;
- C. authorize the use of surveillance footage to aid in the investigation of criminal offenses;
- D. prohibit any personal use of surveillance cameras;
- E. protect and preserve the privacy and constitutional rights of all people; and
- F. abide by the provisions of the City's Surveillance Ordinance and all related state and federal laws, including public records law.

III. DEFINITIONS

- A. *CIMS*: Critical Infrastructure Monitoring System.
- B. *CJIS*: Massachusetts Criminal Justice Information System.

- C. *CORI*: Criminal Record Information System.
- D. *Recording(s)*: Video captured by overt surveillance cameras.

IV. PROCEDURES

A. Purpose

1. Cameras may be deployed to monitor the safety/security of the public by:
 - a. identifying and preventing threats and injury/damage to persons and property;
 - b. identifying, apprehending, and prosecuting criminal offenders; and
 - c. gathering evidence of violations of law in criminal, civil, and/or administrative actions.

B. Management, Control, and Privacy

1. Management and control of the system will be assigned to the Procedural Justice Section.
2. An employee of the department who has reason to review recordings of a particular place and time may send an email request to their direct supervisor who will forward the request to their lieutenant who will then forward the request to the Procedural Justice Section.
 - a. The commanding officer of the Procedural Justice Section will ensure the proper maintenance of a database log of such requests to include the date of time of each request, the person making the request, and the purpose for the request.
3. CJIS and CORI policies, rules, and regulations shall apply to all captured video content.
4. The system may not be used to capture personal identifying information such as cell phone numbers and social security numbers.
5. An employee shall not use cameras to gather intelligence information based on First Amendment-protected speech, associations, or religion.
6. An employee shall not:
 - a. make copies of any recordings;
 - b. erase, alter, or tamper with recordings;
 - c. capture a screen shot of recordings for their personal use, including utilizing a recording device such as a phone camera or secondary video camera to record such.
7. Employees shall not post any recording on any social media site. Public dissemination shall only be authorized by the Commissioner through the Director of Communications and Media Relations. Employees shall only use/access recordings during their official duties.
8. The department shall not utilize any biometric technology, such as facial recognition, to conduct searches of video files or passive searches of the public. Stored video and audio data from a camera shall not:

- a. be used to create a database of photos;
 - b. be used as fillers in photo arrays; or
 - c. be searched using facial recognition software.
 - d. Exception: This section does not prohibit sworn members from using recognition software to analyze the recording of a particular incident when a sworn member has reason to believe that a specific suspect or person in need of assistance may be the subject of a particular recording. The exception must be approved by the sworn member's direct supervisor.
9. The Public Safety Surveillance Camera system is used for official law enforcement purposes only. Anyone who engages in an impermissible use of the Public Safety Surveillance Camera System may be subject to criminal prosecution, civil liability, and/or discipline up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.
10. The Public Safety Cameras will not be used:
 - a. to view, record, or transmit images and/or video at any location or on any property at which a person has a reasonable expectation of privacy; unless the department has the consent of the owner or occupant, a warrant or court order, or objectively reasonable grounds to believe someone is in danger of death or serious bodily injury;
 - b. to target a person based solely on individual characteristics, such as but not limited to race, ethnicity, national origin, disability, gender, sexual orientation, or their First Amendment-protected activity; or
 - c. to harass, intimidate, or discriminate against any individual or group
- C. Release of Recorded Content
 1. Content may be released to the Office of the District Attorney for mandatory discovery in criminal prosecutions and through proper legal process in civil matters, such as court orders and subpoenas.
 2. Content may be released to members of the public and pursuant to public records law.
 3. Content may be released to outside law enforcement agencies pursuant to public records law unless there are exigent circumstances vital to public safety.
 4. Requests must be for a specific date, time period, and place, not for the purposes of scanning an extended time period.
- D. Recordings as evidence.
 1. The Property and Evidence Unit is responsible for storing and maintaining records of all recordings that are physically booked into evidence.

2. Redactions to recordings shall only be made by those persons authorized by the Police Commissioner or their designee.
- E. Equipment maintenance and inspection procedures.
1. The maintenance and installation of the Public Safety Surveillance Camera system is administered by the CPD Public Safety Information Technology Unit. After the data is recorded it is under the administration of the Procedural Justice Section.
- F. Recordings shall only be downloaded and copied by members of the Procedural Justice Section. CPD requests for archived Public Safety Surveillance Camera video shall only be accepted via an internal request email to the Procedural Justice Section. That request will be logged and processed once it is received. The Commanding Officer of the Procedural Justice Section is the keeper of records for all requests made via the Department email as well as subpoenas
1. The Commanding Officer of the Procedural Justice Section shall be responsible for auditing all Public Safety Surveillance Camera requests.
- G. All requests for Video Surveillance footage will be kept in a log by the Procedural Justice Section identifying the date and time of the request, the Requestor, Reason for the request, and Incident Type.
1. A quarterly audit will be performed by the Procedural Justice Section Commander.
- H. Training Requirements
1. Employees of the police department engaged in the various functions of the system will be briefed on its use by the vendor.