





POLICIES AND PROCEDURES MANUAL

	CENTRAL RECORDS	
	POLICY NUMBER: 82-1	ISSUING AUTHORITY 
	EFFECTIVE DATE: June 12, 2025	Christine A. Elow Police Commissioner

I. GENERAL CONSIDERATIONS AND GUIDELINES

Many police activities result in the creation of some type of record, either paper or electronic. Subsequently, there arises the need to manage, secure, store, retain, or destroy records in the custody of the department. The records function is essential for the effective delivery of services to the community and to meeting the management, operational, and information needs of the department.

The issues addressed in this policy are principally concerned with the administration, field-reporting, and central records activities and do not address the secondary records activities attendant to functions in other areas of the department. Additionally, the authorized dissemination of central records, retention schedules, and purging of files are regulated by law.

II. POLICY

It is the policy of the Cambridge Police Department to:

- A. provide an effective and secure central records function that is guided by policy and law;
- B. protect the confidentiality of sensitive records such as those of juveniles, domestic violence and sexual assault cases;
- C. retain or destroy records in its custody in accordance with best practices and law;
- D. release records to the public in accordance with public records law; and
- E. release records to other law enforcement agencies only with authorization from an appropriate supervisor.

III. DEFINITIONS

- A. *ARMS*: Automated Records Management System.
- B. *CORI*: Massachusetts Criminal Offender Record Information, a criminal record check (CORI), provides information to police departments on available Massachusetts arraignments. This type

of criminal record check is done by submitting the name and date of birth for a person. That information is then searched against Massachusetts court records to determine if there is a possible record for that person. This type of criminal record check contains only Massachusetts information and is not fingerprint supported.

- C. *Public Record*: All books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by a governmental entity unless such materials or data fall within one or more of the exemptions found within M.G. L. c. 4, § 7(26) or other legally applicable privileges.

IV. PROCEDURES

A. 82.1.1 (M) Privacy and Security

1. Security of and controlling access to agency files are managed as follows.
 - a. Police incident reports and other department records are securely stored electronically in the Automated Records Management System.
 - b. Paper records are archived in the Records Unit. Only authorized personnel have access to these records by card swipe.
 - c. Electronic records marked confidential have additional security measures with access limited to authorized personnel only.
2. Records files are accessible to authorized operations personnel after regular business hours.
 - a. A master key is securely stored in the Shift Commander's office.
3. The release of agency records is managed according to law.
 - a. The release of agency records may be requested in-person or electronically through email or a phone call. The release of agency records is maintained by the following.
 - (1) All public requests are reviewed and authorized by personnel in the Records Unit, unless there are circumstances that require a supervisor to authorize such release.
 - (2) Requests made by government agencies are reviewed and authorized primarily by personnel in the Records Unit and authorized personnel in units these agencies are specifically requesting records from.
 - b. Government agencies usually can receive records unredacted; records released to the public are typically redacted. Redactions are made on a case-by-case basis, including but not limited to information pertaining to healthcare and medical records, personal, or suspect information.
 - c. Release of records requiring a high level of confidentiality, such as those regarding domestic violence, CORI, and cases under investigation, is generally restricted. Certain

records that can be released are controlled by state law, such as records released to victims.

- d. The department does not require personnel to keep documentation of record requests, and the establishment of such tracking sheet is at the discretion of each unit.

B. 82.1.2 (M) Juvenile Records

1. Guidelines for collecting, disseminating, and retaining juvenile records include the following.
 - a. Methods to distinguish juvenile records include the following.
 - (1) When a juvenile is arrested and booked, there is a checkbox for classifying the incident report as a juvenile record. After entering the date of birth on the booking sheet, the booking officer scrolls down and selects the tab for juvenile.
 - (2) A juvenile record must be marked as such and managed with strict confidentiality; only authorized personnel in the department have access to booking and incident reports that are marked either confidential or juvenile.
 - (3) Any release of information to the public must be directed to the Records Unit, unless there are circumstances that require a supervisor to authorize such release.
 - b. Fingerprints, photographs, and other forms of identification are handled as follows.
 - (1) Fingerprinting and photographing of juveniles are conducted electronically and automatically sent to the state. Within a specified time, confirmation will be received from the state regarding the identification.
 - (2) Photos are captured at booking and retained in the Automated Records Management System. Older paper photos have been securely archived in Crime Scene Services. These date from before the electronic system was installed.
 - (3) All fingerprint records are submitted and stored via LiveScan and subsequently entered in the AFIS database. The actual hard copies are stored in Crime Scene Services in a locked room with limited access by key only.
 - (i) Records can be searched via the AFIS fingerprint station that only authorized personnel have access to. The following is a list of the personnel authorized to access the Crime Scene Services Unit: Crime Scene Services personnel, the lieutenants and deputy superintendent assigned to the Criminal Investigations Sections, the deputy superintendent assigned to the Administrative Services Section, the Superintendent of Support Services, the Police Commissioner, the Shift Commander, and the Facilities Manager in case of an emergency. Physical security and controlling access to juvenile confidential information is handled as follows.
 - (4) Only supervisors and authorized personnel have access to confidential reports.

- (5) The only hard copy related to a juvenile is a Missing Juvenile Report; that report is submitted to the Detective Unit and to the Records Unit. These hard copies are marked as juvenile records.
- c. Disposition of juvenile records after reaching adult age is handled as follows.
 - (1) Whenever a juvenile reaches the adult age of eighteen (18) years old, juvenile records will retain their classification while any new arrest will be processed as an adult arrest.
 - (2) Juvenile records and reports are confidential, and disclosure is permitted only by court order, unless the individual seeking disclosure represents a party or has otherwise been appointed on the case regarding which they seek the disclosure. Reports that are released by the court as permitted or ordered shall not be further copied or released without the permission of the court.
 - (3) Expungement of juvenile criminal records are governed by Massachusetts General Law Chapter 276 §§100F – 100K, and not the Cambridge Police Department. There are “time-based” and “reason-based” reasons for expungement.
- d. Expungement, when ordered by the courts, is managed according to law.
 - (1) The court could order all records regarding a juvenile to be expunged. This is a rare occurrence, and the department will respond according to law when and if it does happen.
- C. 82.1.3 (O) Records Retention Schedule
 - 1. The department follows the state recommended records retention schedule but typically retains records for an additional 1-3 years above what the law requires.
- D. 82.1.4 (O) Crime Reporting
 - 1. Procedures for collecting and submitting crime data to the national or state reporting system are as follows.
 - a. It is the responsibility of the Crime Analysis Unit to provide reports to national databases.
 - b. The Automated Records Management System includes a NIBRS report submission section. This section provides the ability to run a validation report, which indicates errors that must be fixed prior to submission.
 - (1) The senior crime analyst reviews the errors and fixes them.
 - (2) The analyst also identifies and fixes errors that do not appear in the validation report.
 - c. The system also generates a file suitable for submission that the analyst then uploads to the state website, which is subsequently used for transferring submissions to the FBI.
 - d. The state reviews the submission for errors and the analyst then fixes any errors in a timely manner.
 - e. Once the state confirms completion, they submit the report directly to the FBI.

- f. The department no longer submits UCR reports. However, the department does conduct a similar process for internal use, such as the development of directed programming to address hate crimes and other special circumstances.
- E. 82.1.5 (M) Report Accounting System
 1. Procedures to account for the status of reports, to include the complaint control recording and field-reporting systems are as follows.
 - a. For each incident, the Emergency Communications Department generates a CAD number that is entered into the Automated Records Management System; that number is assigned to the case and the subject throughout any future police activity. These numbers are based on the year the incident was reported.
 - b. ECD generates a CAD number for every call; however, not every call results in an incident report. When the officer determines that a call for service will require an incident report, the officer will request an incident/file number from ECD. This is the number that is assigned to the incident, including if the incident needs follow-up investigation.
- F. 82.1.6 (M) Computer File Backup and Storage
 1. The department maintains security of central records computer systems to include the following.
 - a. Data Back-up
 - (1) Computer file backup and storage is conducted with the *Veeam* software system, which consists of disk storage located in a data center within the Robert W. Healy Public Safety Facility.
 - (2) The backup system stores 180 days of history. There is no purging of data.
 - (3) In addition to the separate *Veeam* backups, there is a redundant backup database.
 - (4) Additionally, the computer files for the department ARMS are replicated across separate physical servers and storage systems located in two data centers on different floors within Robert W. Healy Public Safety Facility.
 - b. Storage
 - (1) The department does not use an outside vendor for its electronic data storage; all data is owned and stored locally by the City of Cambridge. The issues for this standard shall be addressed by the City of Cambridge Department of Information Technology. These issues include:
 - (i) data ownership;
 - (ii) data sharing, access and security;
 - (iii) loss of data, irregularities and recovery;
 - (iv) data retention and redundancy;

- (v) required reports, if any; and
- (vi) special logistical requirements and financial arrangements.

c. Access Security

- (1) Physical access and security meet CJIS requirements and is audited on an annual basis. There are card readers and cameras that monitor the data centers. The access cards are reviewed on an annual basis. The camera history is stored for 30 days.
- (2) System access is limited to IT staff only. Data storage is located on an isolated network. User file access is restricted by group membership.

d. Password Audits at Least Annually

- (1) User accounts are reviewed on an annual basis to ensure proper access.
- (2) The passwords are associated with user accounts and the system requires strong passwords per CJIS standards.

G. 82.2.1 (M) Field Reporting System

1. The field-reporting system includes the following.

a. Reports must be written in accordance with the following procedures.

- (1) Officers shall complete an entry into the report-writing system in the ARMS usually before the end of a shift unless authorized by a supervisor to complete the report later.
- (2) Reports shall be completed for arrests, uses of force, and all incident reports as described in section H below.

b. Forms to be used in field reporting include the following.

- (1) Officers shall use the electronic incident report system and may include a supplemental report if needed.
- (2) For hazardous material exposure, officers may use a separate Hazard Exposure Form that is submitted to the City.
- (3) The forms most often used in the field are Missing Persons Reports, Medical Examiner Reports, and Stolen Motor Vehicle Reports.

c. Information required in field reports includes the following.

- (1) Officers shall include all pertinent information regarding the incident and all involved parties, such as subjects, witnesses, and victims.

d. Field reports shall be completed in the following manner.

- (1) Officers take field notes and write reports using either a Mobil Data Terminal in the cruiser, at a report-writing station in headquarters, or at a designated substation.

- e. Procedures for submitting, processing, and supervisory review of field reports include the following.
 - (1) Officers shall notify a supervisor upon the completion of the report.
 - (2) Supervisors then review the report and either reject or approve it; if rejected, the officer will edit and resubmit the report.
 - (3) Depending on the nature of the report, a detective supervisor or FSJS supervisor will determine the follow-up procedures and make any necessary notifications.

H. 82.2.2 (M) Reporting Requirements

1. The department requires a response to every incident in the following categories if the incident is alleged to have occurred in the department's service area:
 - a. citizen reports of crimes;
 - b. citizen complaints regarding police service;
 - c. incidents resulting in an employee being dispatched or assigned;
 - d. criminal and noncriminal cases initiated by law enforcement employees; and
 - e. incidents involving arrests or summonses; generally, citations do not require report documentation.
2. Officers are required to complete an incident report for one or more of the following types of incidents according to department reporting procedures.
 - a. Arrests, including warrant arrests.
 - b. Persons taken into Protective Custody when they are going to be detained at the police station. Officers will complete a police report in these situations whenever there are extenuating circumstances, or when directed to do so by a supervisor;
 - c. Incidents when an officer engages in an investigative detention (apart from a motor vehicle stop for a motor vehicle violation, unless the situation involves an arrest or when in the officer's discretion it is prudent to complete a police incident report).
 - d. Any report of criminal activity or other violation of the law or municipal code, or when there is an indication that a person or persons may be engaged in criminal activity, regardless of whether the victim is desirous of having a police report filed.
 - e. Motor vehicle crashes in which case the report will be filed on the Commonwealth's *Motor Vehicle Collision Report* in the following situations:
 - (1) where the damage to any one vehicle exceeds \$1,000 or there is an injury to any person;
 - (2) whenever the parties involved in the crash are insistent that a police report be completed;

- (3) whenever the collision involves a pedestrian or bicyclist (regardless of whether there are any injuries);
 - (4) whenever the vehicle must be towed from the scene as a result of the collision or for evidentiary purposes; or
 - (5) whenever in the judgment of the officer and/or their supervisor, it is deemed prudent to do so.
- f. In addition to filing a crash report, officers must complete an incident report if any of the following circumstances apply when responding to a motor vehicle crash:
 - (1) Whenever there is injury to any person;
 - (2) Whenever the collision involves a pedestrian or bicyclist (regardless of whether there are any injuries);
 - (3) Whenever a criminal offense has occurred (ex. Leaving the scene of a crash, operating under the influence, negligent operation, etc...)
 - (4) Whenever in the judgment of the officer and/or their supervisor, it is deemed prudent to do so.
- g. Any incident that results in the search of a vehicle or a building (unless the search of building was in response to an alarm, where the officers have found everything to be in order, in which case that information should be made part of the CAD entry);
- h. Statutorily required reports, to include the following types of incidents or situations:
 - (1) domestic violence;
 - (2) identify theft;
 - (3) child abuse;
 - (4) elder abuse and neglect.
- i. Any time an officer is required to take possession of property, to include situations involving stolen, found, recovered, contraband, and evidentiary property.
- j. Any time a situation cannot be resolved at the time when the officer initially intervened, and there needs to be follow-up action at some later time, either by that officer or another.
- k. Any time an officer believes there are extenuating circumstances that make a CAD entry inadequate. This includes those incidents where it appears the individuals have been involved in an interaction with the police and the outcome does not appear to have satisfied the parties involved.
- l. Any time an officer believes that the documentation of the incident, including all activities and actions by the officer, serves as a protective measure.

- m. Incidents where, in the opinion of the officer or supervisor, a written report is necessary.
 - n. For any mental health call that results in a voluntary or involuntary hospitalization or mental health interaction, shall be documented in a report.
 - o. When an officer is in doubt about whether a police report is required, the officer should consult with their direct supervisor.
- I. 82.2.3 (M) Case Numbering System
- 1. Whenever it is determined that an incident requires a case number, ECD will assign that number in sequence according to year. Each case shall have a unique number assigned, which will stay with the case through all subsequent activity.
 - 2. Case numbers will not be duplicated or omitted.
- J. 82.2.4 (O) Report Distribution
- 1. Procedures for the distribution of reports and records.
 - a. Every incident report is stored in the Automated Records Management System. Reports may be directed to department units that conduct follow-up as necessary.
 - (1) There is no internal distribution system. All reports are in the ARMS and all authorized personnel can access them when needed.
 - (i) For internal documentation, once an officer writes a report and it is approved by the supervisor, the report is stored in an electronic journal where it is available for review by users throughout the department.
 - (ii) Users with varying needs have different access for different purposes. Access is determined by rank or job function.
 - (iii) Reports and records may be accessed in various ways including by type or date. Users can retrieve records according to their needs.
 - (2) The Records Unit handles distribution of certain reports to the public, such as accident reports for insurance and incident reports to victims of crime; any request from the public is directed to the Records Unit, unless there are circumstances that require a supervisor to authorize such release.
 - (3) Certain reports are in paper form, such as parking citations, missing persons reports, sudden deaths, stolen vehicles, and 51A reports; these are distributed by request.
- K. 82.2.5 (M) Reports by Phone, Mail, or Internet
- 1. Generally, reports may be filed with the department by phone, or in-person.
 - 2. The Emergency Communications Department maintains a list of Telephone Reporting Eligible Call Types. If a citizen reports a crime by phone, the dispatcher will determine the appropriate

response. Either the report will be taken over the phone or an officer may be dispatched to the location.

3. *TeleServe* is a service the department offers for taking reports over the phone.

L. 82.3.1 (M) Master Name Index

1. The department maintains an alphabetical master name index of persons identified in field reports; the index serves as a cross-reference to all documents in which a person is named.
 - a. This is a sub-section of the Automated Records Management System.
 - b. Personnel authorized to access the ARMS also have access to the master name index and can conduct a search.
 - c. Typically, the index includes the names of victims, complainants, suspects, persons arrested, and witnesses.

M. 82.3.2 (O) Index File

1. The department maintains records to include:
 - a. service calls and crimes by type;
 - b. service calls and crimes by location; and
 - c. stolen, found, recovered, and evidentiary property files.

N. 82.3.3 (M) Traffic Records System Collision

1. The department maintains a traffic records system containing:
 - a. traffic collision data;
 - b. traffic enforcement data; and
 - c. roadway hazard information.

O. 82.3.4 (M) Traffic Citation Maintenance

1. Procedures for maintaining records of traffic citations include the following.
 - a. Citations and other traffic forms including Tow and Inventory Forms, City Ordinance Violations, Traffic Citations, and Parking Citation are stored in a secure closet in the Traffic Unit. Officers can sign out books from the Traffic Unit as needed.
 - (1) A member of the Traffic Unit, usually a sergeant, is designated as the person in charge of maintaining the records, managing inventory, and ordering additional books from the Registry or printer when needed.
 - b. Citations are accounted for through a sign-out system.
 - (1) Officers can obtain citation books by going to the Traffic Unit and signing them out.

- (2) A voided citation must be handled according to the procedures written and promulgated by the RMV.
 - c. New citations and other traffic forms are secured in the Traffic Unit with only authorized personnel having access.
 - (1) Once issued, all citations are submitted to the Records Unit for entry into the secure Automated Records Management System.
 - (2) The paper citations are held for at least one year beyond the time required according to the state records retention schedule.
- P. 82.3.5 (O) Operational Component Record
- 1. Records to be maintained in agency operational components include the following.
 - a. Records of sexual assaults, homicides, and confidential informants are filed in the Criminal Investigations Section.
 - b. Personnel and Professional Standards Unit records, such as Internal Affairs investigations, are stored in their respective units.
 - c. The Domestic Violence Unit may keep case notes which are only available to certain authorized personnel.
- Q. 82.3.6 (M) ID Number and Criminal History
- 1. The department assigns an identification number and maintains a criminal history file for each person arrested. These numbers are cross-referenced with persons arrested and are stored electronically in the Automated Records Management System.
 - a. Each person who has been arrested is assigned one unique number regardless of the number of times arrested. If an officer fails to confirm the correct spelling of names, or there are other problems, an additional number may be assigned.
 - (1) However, the goal is to have one number for each person. The Crime Analysis Unit often merges ID numbers so that one person only has one ID number.
 - b. Numbers are assigned electronically and sequentially with no numbers omitted. However, these numbers may not stay in sequential order for persons arrested due to input errors.
 - c. The file may include fingerprints, criminal history reports, photographs, and a copy of arrest reports unless these are cross-referenced and available through other systems.