



Somerville Police Department 	TYPE: GENERAL ORDER		POLICY NUMBER: 415				
	Subject: Records Management						
	Issuing Authority: David Fallon Chief of Police		Signature: 	Effective Date: January 17, 2018			
		Number of Pages: Page 1 of 8					
Accreditation Standards (5th Edition) 72.1.3, 82.1.1, 82.1.2, 82.1.3, 82.1.7, 82.3.5, 82.3.6		<input type="checkbox"/> New <input checked="" type="checkbox"/> Revised <input type="checkbox"/> Amended					
Revision & Reissued Dates:	1/18/16						

Purpose

Many of the activities in which police personnel are involved result in the creation of some types of records. Although the records are created by and in the custody of this department, they are actually under the authority of the Massachusetts Secretary of the Commonwealth, Public Records Division. The length of retention is determined by that office, and they may lawfully be destroyed only with the permission of that office.

The purpose of this directive is to establish organization and guidance for the collection, storage, and permanent archive or destruction of records.

Policy

It is the policy of the Somerville Police Department that:

- A. C.O.R.I., juvenile records, and personal data will be protected in compliance with Massachusetts General Law, C.M.R.s and other regulations.
- B. All records in the custody of the department shall be retained and/or destroyed in accordance with the standards of the Office of the Secretary of the Commonwealth.

Definitions

C.O.R.I.: “Criminal offender record information”: records and data in any communicable form compiled by a criminal justice agency which concern an identifiable individual and relate to the nature or disposition of a criminal charge, an arrest, a pre-trial proceeding, other judicial proceedings, sentencing, incarceration, rehabilitation, or release. For a more in-depth definition, see the department policy on C.O.R.I.

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 any officer or employee or any agency, executive office, department, board, commission, bureau, division or authority established by the General Court to serve a public purpose, unless such materials or data fall within one or more of the exemptions found within M. G. L. Chapter 4, Section 7(26).

Procedures

1. Administration: The Administrative Captain is responsible for the records management function. He/she directly supervises the Records Clerks whose duties shall include:

- A. Collection of all reports and related data
- B. Distribution of reports to appropriate agency recipients
- C. Maintenance of incident, accident, arrest, and other reports in an organized manner through filing of hard copies and management of electronic records
- D. Retrieval and distribution of records and documents for authorized persons and entities
- E. Compliance with records requests under state law and the Freedom of Information Act
- F. Protection of C.O.R.I., confidential and personal data
- G. Maintaining the archive of records required to be stored permanently
- H. Destruction of records in compliance with protocols provided by the Secretary of the Commonwealth

2. Storage and Security [82.1.1(a)]

A. Paper Records:

- 1. The Records Clerks are responsible for the security of paper records stored by the department. All paper records shall be stored in locked file cabinets.
- 2. Paper records are stored in the Records Bureau and the Administrative Captain's Office in locked file cabinets in key card access controlled offices.
- 3. Paper records shall be stored in a secure area free from unsupervised access by members of the public and unauthorized personnel locked file cabinets in key card access controlled offices.

B. Electronic Records:

- 1. In order to ensure confidentiality of all police intelligence, the in-house computer system is password protected. Only employees with a proper username and password

may log onto the system. In addition, each employee is allowed access to only those sections they have a need to access based on their function. For instance only specific personnel are allowed access to sex assault files and only CORI certified employees will have access to offender data.

2. Security of electronic records shall be the responsibility of System Manager. For further information about electronic records, see the department policy on Computers and Data Security.

C. Paper Records Stored by Operational Components: Security of records stored by other operational components of this department shall be the responsibility of the supervisor of that component. The following records are stored in locked file cabinets within locked offices with controlled access: [82.3.5]

1. Sexual Crime Records are stored in the office of the Family Services Unit.
2. Sexual Offender Registry files are stored in the Family Services Unit.
3. Homicide Investigation files are stored in CID.
4. Records of complaints against department employees are stored in the Professional Standards Office.
5. Juvenile records are stored in CID in individual detectives locked file cabinets. Key card access to CID is limited to Detectives and Superior Officers [82.1.2(c)]

D. Access by Employees [82.1.1(b)]

1. Paper records stored by the records management section shall be accessible to employees during business hours.
2. Requests for records may be made in person during business hours at the Records Window.
3. Paper records may not be obtained after business hours.
4. Electronically stored records to incident reports, arrest reports, and master name files, are available to authorized personnel twenty-four hours a day through the department's computer network which is password protected. For further information about electronic records, see the department policy on Computers and Data Security.

3. Records/Reports Distribution and Security [82.1.1(c)] [72.1.3]

- A. Department records/reports maintained in the Records Bureau will not be open to public view within that designated area. No visitor, whether on official or unofficial business,

shall be allowed to enter the Records Bureau for the purpose of viewing any department records, nor shall any officer, clerk, or other employee allow or condone this act.

- B.** Only members of the department shall have access to the Records Bureau. All electronic records, if legally accessible and individual password protected, shall be available at all times in order to facilitate investigations and other duties being performed by officers of the department. All officers, particularly Shift Supervisors, shall familiarize themselves with the locations of various types of electronically stored information so that retrieval of records will be quick and efficient.
- C.** When reports, photos, or evidence are required for court, the officer will ensure that they are kept in a secure manner out of public view to maintain confidentiality. All reports, photos or evidence will be returned to the appropriate department function at the conclusion of court for disposition.
- D.** Manipulation or alteration of existing software running on department owned mobile, desktop, or handheld computers is prohibited. Due to the threat of data corruption, any files or software that originate from outside the department should be analyzed by the System Manager before being installed/accessed on department equipment.
- E.** In order to ensure data integrity and security, the System Manager will install the appropriate software, security, patches, and updates. Recognizing that these in themselves do not guarantee complete security, all personnel will abide by the department's policy on Computers and Data Security. [82.1.7]

4. Release of Records to Government Agencies [82.1.1(c)] [82.1.7] [82.1.2]

- A.** Requests for police reports from a government agency are authorized for any lawful purpose, and subject to C.O.R.I. restrictions, if the request is made in writing or in person from an authorized government official with proper identification.

5. Release of Records to Non-Governmental Agencies [82.1.1(c)]

- A.** Requests for police reports from civilians, attorneys, and insurance companies will only be released (subject to C.O.R.I.) under guidelines authorized by the Administrative Captain.
- B.** All requests are handled by the Records Bureau. Any incident pending investigation or otherwise exempt from the public records law will not be released. Any report containing personal identifying information of witnesses and/or victims will be sanitized before distribution. A fee shall be charged for copies of reports. All money received at the Records Bureau is submitted weekly to the Treasury Department at City Hall.

6. Juvenile Records

- A. All persons arrested are processed using the QED software system, which is individualized password protected. The Booking Officer performing the booking procedure chooses whether the person being booked is classified as an adult or juvenile. Even if an incorrect designation is chosen, QED is automatically able to sort juvenile arrestees from adult arrestee using the date of birth provided by the arrestee. Juvenile arrestees are not recorded in the Booking Log. [82.1.2(a)]
- B. The department uses an Offender Based Tracking System and assigns an identification number and matching criminal history file for every arrest. Digital photographs and fingerprints are taken of all persons who are arrested. Photographs are stored in QED, and fingerprints are maintained electronically in AFIS. [82.1.2(b)] [82.3.6]
- C. Juvenile records for active or recently closed cases involving juveniles may be stored by individual detectives in locked files cabinets in key card access controlled CID. Any information that is stored in the digital format is password protected and controlled. Access to juvenile records is limited to personnel who have a legal right to this access. [82.1.2(c)]
- D. Juvenile records shall be maintained as such after an individual has become an adult. [82.1.2(d)]
- E. No juvenile records shall be disseminated without the approval and authorization of the Chief of Police, his/her designee or the District Attorneys Office. [82.1.2]

7. Challenge of Accuracy of Police Records

- A. **Police Reports:** Any person who wishes to challenge the accuracy of a police report may do so by:
 - 1. Speaking with a supervisor to explain the nature of the alleged inaccuracy
 - 2. Submitting a request in writing explaining the nature of the alleged inaccuracy
- B. The employee's supervisor will present the request to the employee who authored the report, or portion of a report in dispute.
- C. The author will review the portion in question. The report's author may:
 - 1. With the assistance of the System Manager, edit the report to correct the inaccuracy raised or any other inaccuracy found
 - 2. Take no action
- D. Upon completion of this process, the involved supervisor will advise the person challenging the report in writing of the outcome of the review.

- 8. Expungement:** This procedure shall apply to adult and juvenile records.
- A. Upon receipt of a judicial order of expungement of any record, records management personnel shall identify and obtain the record. [82.1.2(e)]
 - B. Hardcopy records shall be destroyed in compliance with this policy.
 - C. Electronic records, files, and other data will be deleted manually or using specific deletion software programs in the department's records management software.
- 9. Retention of Records [82.1.3]**
- A. Police department records shall be retained, at a minimum, for the time specified in the records disposal schedules promulgated by the Secretary of the Commonwealth, as amended from time to time.
 - B. Massachusetts General Laws Chapter 66, Section 8, provides that the Supervisor of Public Records, a branch of the Secretary of State's Office, has the authority to develop disposal schedules which designate the lengths of time which various records must be maintained by a police department. The statute further provides that such records may be destroyed only with the written approval of the Supervisor of Public Records. It should be noted that the statute applies not only to documents which are defined as **public records**, but also to any "written or printed book or paper, or any photograph, microphotograph, map or plan."
 - C. It shall be the responsibility of the Administrative Captain to ensure that all-legal requirements regarding the retention of records be adhered to, and to supervise and control the process of disposal of these records when necessary.
 - D. Disposal schedules apply to information, not the media containing the information. If records maintained on electronic media are printed out in an eye-readable format, the original electronic records may be immediately destroyed.
 - E. If the electronic record is the sole source of the information, it must be treated in the same manner as its hardcopy counterparts for the purposes of disposal, and must be maintained in accordance with the disposal schedule.
 - F. Therefore, virtually every document in the custody of the Department must be retained in safekeeping for the period of time specified in the "Retention Schedule", or until permission for destruction is obtained by the Supervisor of Public Records.
 - G. Documents that are not classified as Public Records must be retained for a period of seven (7) years.

H. It shall be the responsibility of the Administrative Captain to ensure that all-legal requirements regarding the retention of records be adhered to, and to supervise and control the process of disposal of these records when necessary.

10. Destruction

A. Obtaining Authorization

1. Nearly all records held by police departments require authorization of the Supervisor of Public Records, Office of the Secretary of the Commonwealth. Instructions and sample letters are included in each category of Records Disposal Schedule which is available from the Secretary of the Commonwealth's web site: [Massachusetts Secretary of State](#)
2. Any records which may be destroyed without the permission of the Supervisor of Public Records shall be destroyed after being retained at least for the minimum duration specified in the destruction schedule. Such records are denoted with an asterisk "*" on the destruction schedule.
3. Police department records shall be destroyed in compliance with the records disposal schedules promulgated by the Secretary of the Commonwealth, as amended from time to time.
4. No records that are subject to any current or pending litigation, public records request, or which have not been retained for at least the minimum retention duration may be destroyed.
5. Original records cannot be destroyed without the written permission of the Supervisor of Public Records.
6. No records created prior to 1870 may be destroyed.
7. Application for Authorization for Destruction: Submit a letter in duplicate to the Supervisor of Public Records requesting permission for destruction. A sample letter is available in the Forms Section at the end of the Secretary of State's Municipal Records Retention Manual. The letters must be signed by the Chief of Police and contain the following:
 - a) Schedule Number: the destruction schedule number in which the record to be destroyed is found (Police Department: 14-81)
 - b) Date of last revision of the schedule, listed on the Disposal Schedule cover sheet
 - c) Series Number, as indicated on the destruction schedule to identify the particular type of record to be destroyed
 - d) Estimated volume of records to be destroyed

- e) Inclusive dates of each series to be destroyed
 - f) Date of last audit, if applicable
8. Upon approval, one copy of the letter will be returned and the records may be destroyed.
 9. To destroy records that are not included on the police disposal schedule, refer to the Administration/Personnel (23/89) records disposal schedules. This schedule includes records held in common by various municipal offices.
 10. To destroy a record that is not included in the police disposal schedule or the Administration/Personnel (23/89) disposal schedule, submit a letter in duplicate to the Supervisor of Public Records. In addition to the information above, the letter should describe the record. If possible, attach a photocopy of the record.

B. Methods of Destruction:

1. Records containing confidential information or information that would be segregated, excluded, or redacted from release as a public record shall be destroyed in such a manner as to make the record un-readable and unrecoverable. Security of the records must be maintained until they are actually destroyed.
2. Paper records, optical media, and flexible media, like a floppy drive, may be shredded or burned.
3. Hard drives may be destroyed by the following methods:
 - a) Disassemble the hard drive case and destroy the physical disk.
 - b) Run a wipe utility to over-write the disk and file allocation tables.
 - c) Complete degaussing.