ACTON POLICE DEPARTMENT

	DEPARTMENT MANUAL; P&P: Administration	
POLICY & PROCEDURE # 4.14	DATE OF ISSUE: 01/23/2024	EFFECTIVE DATE: 1/30/2024
SUBJECT: RECORDS SYSTEM	ISSUING AUTHORITY: Chief James Cogan	
REFERENCE(S): Massachusetts Police Accreditation Commission # 82.1.1; 82.1.2; 82.1.3; 82.1.6; 82.1.7; 82.2.3; 82.2.4; 82.3.1; 82.3.4	____NEW __X__AMENDS ____RESCINDS	

I. PURPOSE

This directive describes the Department's guidelines with regard to employee access to and disclosure of information contained in the Department's computer system. This includes incident and criminal information on the server systems, mobile data terminals in police cruisers, electronic mail messages, and information contained on the shared network. This directive also addresses records (hard copies) security, storage, and disposition.

II. POLICY

A. It is the policy of the Acton Police Department to maintain a records management system in order to provide reliable information to be used in management decision-making.

The information is important for analyzing workload, determining resource needs, budget preparation, resource allocation, record keeping, employee safety, and other departmental needs. Access to data contained in the system must be controlled in a manner that will ensure only authorized access.

It is also necessary to permit the dissemination of public data to interested individuals. This data must be in conformance with the standards of the Massachusetts Criminal History Systems Board in order that the rights of any individual are not infringed. All information needs to be carefully reviewed prior to dissemination to ensure that it is not restricted.

III. PROCEDURES

A. **Administration**: The records management system (RMS) provides a comprehensive representation of the department's operation at any given point in time, as well as projecting future trends from current and past data.

1. The Chief of Police or his/her designee shall work in collaboration with the Town of Acton IT Department updating and maintaining the information system when needed.

2. Responsibility for recording and/or providing specific types of data is assigned to and/or shared by various shifts or Divisions. Types of data recorded into the system include, but are not limited to the following:

   a. Calls for service
   b. Arrest bookings
   c. Incident report narratives
   d. Trespass lists
   e. Stolen property
   f. Alphabetical master name index **[82.3.1]**
   g. Offender history
   h. Collision data
   i. Juveniles
   j. Emergency notification list
   k. Alarms
   l. Business directory
   m. Street files
   n. Digital photos

B. **Records**: All arrest reports, incident reports, summons, motor vehicle violations, criminal history transcripts, digital photographs, and various other records are entered in the Department records management system. These records are assigned a unique and sequential incident number. These records are password protected and may be accessed by authorized Departmental personnel from any network computer, and are available 24 hours a day. All criminal investigation reports requiring follow-up are routed to the Special Services Division. All other reports requiring follow-up will be forwarded to their respective Departmental operational components (e.g. traffic complaints to the Traffic Unit). **[82.1.1(2A)(2B)(2C)] [82.1.7] [82.2.3] [82.2.4] [82.3.4]**

C. **Privacy and Security Precautions**: The Records Room is secured by electronic card key access. Access is limited to authorized personnel and Division Commanders twenty-four (24) hours a day. The Patrol Division Commander will be contacted for after-hours access. **[82.1.1(2A)(2B)(2C)] [82.1.2(6)]**

D. **Sexual Assault Records Security**: When submitting hard copies of sexual assault incident reports to the Patrol Shift Supervisor for review, the reporting

officer shall secure the sexual assault incident report in the locked bin labeled "Sexual Assaults" located underneath the employee mailboxes in the roll call room. Once secured in the bin, the reporting officer shall notify the Patrol Shift Supervisor of the report status and location. The reporting officer shall complete their initial report prior to the end of their tour of duty.

Upon being notified of a sexual assault report secured in the bin labeled "Sexual Assaults", the Patrol Shift Supervisor shall open the bin and review the incident report. The keys to the bin shall be secured in the Patrol Sergeant's office within the key box.

Once the Patrol Shift Supervisor completes his/her review of the incident report, the hard copy of the report shall be secured back in the bin labeled "Sexual Assaults". The Patrol Shift Supervisor shall notify the Detective Sergeant(s) of the location and status of the incident report for further action.

E. **Juvenile Records Security**: Offender histories for adults and juveniles will be segregated electronically and hard copies physically. Electronic copies will be clearly labeled as "Juvenile" in the records management system. Hard copies of closed incidents shall be filed in the Records Room in red file folders. Open cases shall be filed in a locked cabinet within the Student Resource Officer's (SRO's) office. Access shall be restricted by electronic key card or key to authorized personnel. **[82.1.2(1A)(5)(6)]**

1. The collection of fingerprints and photographs for juvenile offenders shall be subject to the same requirements as adults. **[82.1.2(2)(3)]**
2. Dissemination of Juvenile and adult fingerprint cards, photographs, and reports shall only be to other CORI-approved agencies upon approval of a Division Commander **[82.1.2]**
3. Retention of juvenile and adult fingerprint cards and photographs is required.
4. Juveniles taken into custody for criminal-type offenses shall be subject to the same reporting requirements as adults.

F. **Record Keeping**:

1. Written reports, photographs, and any other forms of identification shall be filed in the locked Records Room. Juvenile records will be kept physically separate from adult arrest records in red file folders. Juvenile reports in the RMS system shall be restricted to authorized personnel only and will be clearly labeled as "Juvenile". **[82.1.2(1A)(5)(6)]**
2. Disposition of Juvenile Records: When a juvenile reaches adult age, any records of activity obtained while a juvenile will remain with any adult record of such an individual. **[82.1.2]**
3. Expungement by the Court: This procedure shall apply to juvenile and adult records.

a. Upon receipt of a judicial order of expungement of any record, records management personnel shall identify and obtain the record.

b. Hard copies shall be destroyed by shredding or burning.

c. Electronic records, files, and other data will be deleted manually or using specific expungement or deletion software programs in the Department's records management software. **[82.1.2]**

G. **Releasing of Department Records**: **[82.1.7]**

1. GENERAL PUBLIC: Members of the public requesting access to department records shall submit a written request form to the Records Clerk. The Records Clerk shall forward the request to the Deputy Chief for approval and dissemination. The Deputy Chief will disseminate records in accordance with the state public records law and with the Criminal Offender Records Information Act (C.O.R.I). **[82.1.1(2D)(2E)]**

   Due to changes in the Public Records Law, the Acton Police Department is required to change the way it responds to public records requests concerning reports of sexual or domestic violence. With the exception of the Records Clerk, no other department member shall release records to the public without authorization from the Chief of Police. If a request to release department records is made the Records Clerk shall remove the following records prior to providing the documents to the requesting party:

   a. All reports of rape and sexual assault

   b. All reports of attempted rape and sexual assault

   c. All reports of abuse perpetrated by family or household members

   d. All communications between police officers and victims of rape, sexual assault, or abuse perpetrated by family or household members

   e. Any police log(s) concerning such reports

2. POLICE DEPARTMENTS/ OUTSIDE AGENCIES: A request received by phone for records from a Police Department or outside agency the Patrol Shift Supervisor is to call back that department or agency and confirm the identity of the caller before the release of any records. After confirmation is made the Patrol Shift Supervisor may disseminate records to any other criminal justice agency appearing on the CORI list in CJIS and any other authorized agency. **[82.1.1(2E)]**

3. NIBRS/UCR Function: The Chief of Police or his/her designee, typically a member of the Department's Communications Unit, shall be responsible for the department's NIBRS/UCR Function. This function includes the collection of the department's crime data, the correction of critical errors, the submission of monthly crime data to the state police, and for correcting of errors found by the state police. **[82.1.4 (1)(2)(3)]**

H. **Photographs**: Photos are stored both electronically in the RMS and in the Records Room. Photographs in the RMS are password-protected, and hard copies are secured in the locked Records Room.

I. **Equipment, Hardware, Software, and Systems**:

1. Adding / Modifying Software & Hardware: No one may add or modify software or hardware without the authorization of the Chief of Police and System Manager(s).

J. **Licensing**: All programs introduced into the system shall be properly licensed.

K. **Computer Access / Security**: Software and hardware have been installed to prevent unauthorized network access. The System Manager(s) will assign access codes (logins) and the initial user's passwords for the department computer network system: **[82.1.6(1)]**

1. Passwords are encrypted and are known only to the users and System Manager(s).
2. Users may not divulge their passwords to anyone without the authority of the System Manager(s).
3. Access codes will be audited to verify all logins.
4. Employees who separate from the Department/Town will have their logins deactivated immediately by the System Manager(s).
5. Logins will be audited annually for verification of all passwords, access codes, and access violations. **[82.1.6(6)]**
6. Logins no longer needed shall be disabled on the system server.

L. **Computer File Backup & Storage**: Records on the department's centralized computer system shall be backed up onto a media device daily by the System Manager(s). The backup devices are stored in a secure room in the communications center as well as a secure room at the town hall. **[82.1.6(2)(3)(4)]**

M. **Use of Department E-Mail & External Internet Services**: All internal e-mail messages whether sent or received by employees and all files located or accessed by departmental computers are considered department records. All external files, including personal e-mails and data that are accessed using departmental computers, are not considered private communications and can be subject to scrutiny and/or disclosure by proper departmental or legal authority.

IV. Records Retention Schedule

The Department shall comply with the Commonwealth of Massachusetts Municipal Records Retention Manual 2018 edition. See hyperlink:

https://www.sec.state.ma.us/divisions/public-records/download/MA_Statewide_Records_Schedule_updated2022-10-31.pdf
[82.1.3] [82.3.4]

RECORDS SYSTEM INFORMATION

History: Manual I, Section III

Updated Policy For Maintaining and Disclosing Records Concerning Sexual or Domestic Violence (Policy 4.33)