INFORMATION SYSTEMS

General Order Number: 12.2 **Effective Date: July 9, 2024**

POLICY:

It is the policy of the Brookline Police Department to maintain an information system in order to provide reliable information to be used in management decision-making.

This is important in predicting workload, determining manpower needs, budget preparation and other resource 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 dissemination of public data to interested individuals, in conformance with the standards of the Massachusetts Criminal Systems History Board, and to the extent that the rights of any individual are not infringed. All information will be carefully reviewed prior to dissemination to ensure that it is not restricted.

PROCEDURES:

A. **ADMINISTRATION**: The Information System provides a comprehensive picture of the Department's operations at any given point in time, as well as providing information for projecting future trends from current and past data.

1. The Records Division, with the assistance of the Technology Division, is responsible for developing, establishing and maintaining a management information system.

2. Responsibility for recording and/or providing specific types of data is assigned to and/or shared by various Divisions or Units as follows:

a. Patrol Division - Calls for service, trespass notices, attendance, arrest bookings, stolen property, names, incident report narratives, vehicles and tows.

b. Records Division- Criminal History, stolen property, names, Uniform Crime Report and National Incident Based Reporting System coding, warrants, evidence/property, summons, subpoenas, personnel, department inventory and emergency notification list.

c. Detective Division - Stolen Property, case narratives, case management, firearm permits/licenses, pawnshop activity, domestic violence abuse orders, juveniles, field interviews, and drug files.

d. Traffic Division – Parking fines, motor vehicle citations, traffic accidents and police details.

e. Training Division – In-Service training records and lesson plans, training bulletins, Brookline Police Department Manual, any additional materials and certificates pertaining to education and training.

f. The Technology Division will share responsibilities for recording calls for service, and any other recording deemed appropriate.

3. The responsibility for reviewing, correcting and reporting of collected data is assigned to the Technology Division, and the respective units/users who entered the data.

B. REPORTS: Reports reflecting comparative data and trends on activities shall be created daily, monthly and annually.

1. The Daily Journal is a computer application, accessible to the public at the front desk, that summarizes Department activities during the previous 24 hours. Specific dates can be summarized upon request.

2. The Department's Crime Analyst shall prepare a weekly report that contains year-to-date data, NIBRS reports, arrests, trends and other timely and pertinent information.

3. Each division commander shall submit a monthly report that contains information relative to activities of their unit for the previous month.

4. The Annual Report shall summarize the monthly reports. This report shall provide comparative data and statistics, and account for the activities of the entire department.

5. DISSEMINATION**:** Monthly and annual reports shall be disseminated to affected organizational units as directed by the Chief of Police.

6. NIBRS CRIME REPORTS**:** The National Incident Based Reporting System (NIBRS) shall be prepared utilizing the UCR/NIBRS application in the CAD System and the F.B.I. NIBRS Reporting Handbook.

7. REPORTING CRIME STATISTICS TO THE STATE: The Brookline Police Department reports statistics to the National Incident Reporting System (NIBRS) and to the Crime Reporting Unit of the Massachusetts State Police. The Records Clerk is responsible for generating the report each month and forwarding it to the Technology Division. The Technology Officer will submit the data to the Massachusetts State Police on a monthly basis.

C. **PowerDMS:** In an effort to promote the dissemination of information within the department, the Department has moved its document storage and management to PowerDMS. PowerDMS is an online document storage platform designed to facilitate seamless document upload and accessibility for review. The platform's interface allows for easy document and topic searches.

a. All Brookline Police Department personnel will receive training on how to use this program.

b. All sworn members of the Department are responsible for checking PowerDMS at least weekly.

c. Division supervisors will ensure that their officers are checking PowerDMS at least weekly and will ensure that any assigned tasks, such as acknowledging polices or assigned trainings are completed.

2. PURGING OF INFORMATION:

a. The Technology Division is responsible for purging the out-of-date information from SharePoint.

D. **DEPARTMENT EMAIL:**

Department Email is the most commonly used way to share information with large groups simultaneously, across shifts and divisions and between ranks. Employees are responsible for checking the Brookline Police email system to see what pertinent information and/or directives have been issued since their last tour. They are responsible for reading and understanding each directive, which has been issued during their absence, whether or not it is read at their roll call or otherwise brought to their attention. For further information on the use of Department Email, please refer to the General Order 21.1 (Communications).

E. **FINGERPRINTS/PHOTOGRAPHS:**

1. Fingerprints shall be taken of all persons arrested, applicants for employment, and certain for licensing purposes.

2. Two cards shall be taken of all employment applicants.

3. Fingerprints of suspects, applicants and other persons will be maintained in the fingerprint file, located in the Detective Division. Cards will be maintained using the modified Henry system of classification.

a. All officers assigned as photographers and/or evidence officers shall have access to the fingerprint system. Request for cards shall be submitted through the Prosecutor/Investigator, any Sergeant or Lieutenant.

b. Fingerprints shall only be disseminated to legitimate law enforcement agencies for lawful purposes.

c. Juvenile fingerprint cards are stamped JUVENILE and are filed separately in the fingerprint card storage cabinet.

d. If fingerprint cards are removed and subsequently turned over to another department or entity, an incident report will be made indicating the officer in charge, the agency and person requesting the cards, reason, time, date, etc. Upon return, another incident report will be made indicating that information.

e. Photographs will be taken of all arrested persons, job and license applicants and will become a permanent record of the Department.

f. Juvenile photographs, like other photographs of individuals, are stored under their master card in the central computer system.

F. RECORDS:

1. RECORD CARDS/Offender History Application: The use of Record Cards was discontinued in 1986 when our criminal history records were computerized. These cards are still available for reference and are available in the Records Department archive.

The Offender History System serves as a permanent record of the police department and may follow a defendant's criminal history through their career. Records Division personnel are to keep information contained in the Offender History System in utmost confidence. Information contained on record cards are to be divulged only by designated personnel in methods that have been approved by the Brookline Police Department.

a. An Offender History shall be initiated for the following reasons; when a crime is committed (felony or misdemeanor), when a criminal motor vehicle offense is committed or when a summons is issued from the court for any reason.

b. An Offender History shall contain the following information; name, address, occupation, social security number, alias, place of birth, date of birth, mother, father, height, weight, complexion, color of eyes, color of hair, date of issue, case number, date of offense, offense, arresting officer, PHC number.

c. Upon order of the court, records shall be expunged by records personnel as directed by that court.

d. Juvenile Records shall be maintained as such after an individual has become an adult. Juvenile records are **separated** from adults in the central records system, though juvenile records for active or recently closed cases may be stored by individual detectives in their own locked file cabinets. These records include but are not limited to: fingerprints, photographs, and other forms of identification pertaining to juveniles. Any information that is stored in a digital format is password protected.

e. Access to juvenile records is limited to personnel who have a legal right to this access. No juvenile arrest information shall be disseminated without the approval and authorization of the Chief of Police or their designee.

f. Access to these records shall be on a "need to know" basis. If access is needed, it shall be authorized by Deputy Superintendent – Records Division or their designee.

2. RECORDS DISTRIBUTION AND SECURITY

a. All Department records are maintained under the overall control of the Chief of Police and shall not be open to any public view.

b. All access to criminal history records that are maintained in the in-house computer system is accessible 24 hours and shall be subject to the same procedures as stored copies in the file system. Any release of computerized records shall be held to the conditions of M.G.L., Chapter 6, Section 172.

c. No information shall be released, given or issued to the news media or to any members of the press concerning the evidentiary aspects of any criminal investigation without the prior approval of the Chief of Police or his or her designee.

d. No record shall be released to the public without the prior approval of a supervisor. Law enforcement agencies must submit a written request on department letterhead.

e. File security is accomplished through username and password protection. The rules and conventions for usernames and passwords differ slightly by system. It is the user's responsibility **not** to share passwords. The user is responsible for any security violations tied to a password.

f. The Technology Officer will perform a quarterly audit to verify password and security access.

g. Once a member of the department's employment has ended, the Technology Officer will delete their passwords and ensure that they no longer have access to the department's computer systems.

h. Paper records will be stored in locked file cabinets by the Records Clerk, and will be housed in an area open only to authorized Department personnel via key card access during normal business hours. Juvenile records will be maintained in separate cabinets from adult records and will be distinguished with a red "JUVENILE" stamp in plain sight.

i. Department records and reports maintained in the Records Division 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 division for the purpose of viewing and Department records, nor shall any member of the Department condone this act.

j. The Brookline Police Records Division provides reports according to the guidelines set by the Massachusetts Public Records Act. Some or all materials requested may be subject to redaction or denial of records in whole, and all requests are subject to review by the Deputy Superintendent-Traffic Division.

k. Reports may not be readily available upon request; by law, the Records Division has ten business days from the date of the request to respond. In most cases, a request can be filled within a few days. If a request is extensive, the requestor will be provided with an estimated timeline that it will take to fill such a request as well as the associated fees.

l. Under the Public Records Law there is no specific form that must be used to make a request, however, members of the public are asked to provide a reasonable description of what is being requested, specifying exactly what materials are to be obtained. The requestor MUST provide contact information. Requests may be submitted by mail, online or in-person during the normal business hours of the Records Division.

G. DATA BACK UP:

1. Data on the department's computer system is recorded by two "mirror image" hard drives.

2. The mirror image is backed up nightly to a third local server as well as to an offsite Azure cloud-based server.

3. The hard drives are stored in the secured Technology Division Office and all data is encrypted and stored in a CJIS compliant manner.

4. The Technology Division is responsible for the maintenance and security of all computer files.