



CRIMINAL INTELLIGENCE

General Order Number: 41.1

Effective Date: June 12, 2019

POLICY:

The Brookline Police Department recognizes the need to maintain the delicate balance between government interests and individual rights in a free society. To simultaneously address these needs and rights requires the adherence of all members of the Department to the following guidelines concerning the gathering, storing and sharing of criminal intelligence.

It is the purpose of this policy to provide Brookline Police Officers, and in particular those Detectives assigned to the Intelligence Unit, with guidelines and principles for the collection, analysis and distribution of intelligence information.

Criminal intelligence concerning an individual or organization shall be collected and maintained by the Department only if there is reasonable suspicion that the individual or organization is involved in criminal conduct or activity and that the information is relevant to that criminal conduct or activity. No information will be submitted to, accepted by, or maintained knowingly in the Department's files concerning political, religious, or social views, associations or activities of any individual, group association, corporation, business, partnership, or other organization unless such information directly relates to an investigation of criminal conduct or activity, and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity and the information could be pertinent.

No information which has been obtained in violation of any applicable federal, state, or local law or Town By-Law shall be included in the Department's files.

Criminal intelligence information acquired by the Department shall be disseminated only where there is a need to know and right to know the information in the performance of a law enforcement activity. This policy is intended to remain at all times consistent with the current language of 28 CFR, Part 23.

DEFINITIONS:

Information: raw data. It is knowledge derived from study, experience, or instruction. It is knowledge of a specific event or situation; news; word.

Criminal Information is the above as it pertains to criminal conduct and or activity.

Criminal Intelligence: records and data compiled by a criminal justice agency for the purpose of criminal investigation, including reports of informants, investigators or other persons, for any type of surveillance associated with an identifiable individual or organization.

Reasonable Suspicion: established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

Need to Know: the requirement that the information requested is both pertinent and necessary for the requesting individual or agency to initiate, further or complete an assigned law enforcement task.

Right to Know: The official capacity and statutory authority for the requesting individual or agency to receive the requested information.

Strategic Intelligence: That intelligence material that tends to support long range planning.

Tactical Intelligence: That intelligence that tends to assist immediate law enforcement needs and support short-range planning.

Dissemination of criminal intelligence information: Except as noted in the below paragraph, intelligence information shall be disseminated only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

The above paragraph shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

Concerning criminal intelligence information: All criminal intelligence information shall be entered into and maintained within the Department's Larimore Intelligence System. The Department shall adopt administrative, technical, and physical safeguards (including audit trails) to insure against unauthorized access and against intentional or unintentional damage to this information.

The Department shall have criteria by which to purge information from the files which has no relevance or importance. Material purged will be returned to the submitting agency or confidentially destroyed by the best means available. No record of the names of individuals, organizations, etc., that are purged will be maintained by the Department.

The Department shall have sanctions to control unauthorized access, utilization, or disclosure of information from the files.

The Chief of Police shall ensure that all members of the department adhere to this policy and other Department policies, procedures, rules and regulations. The Chief of Police shall enforce this policy and act as the Department Head for all disciplinary and enforcement actions for any violations of it by department personnel. The Department will utilize all legal means available to protect criminal intelligence and criminal intelligence information obtained from outside agencies.

The Department recognizes that individuals and/or organizations will commit crimes against society. The Department is obligated to investigate crimes against society, and bring the investigation to a successful conclusion by bringing the perpetrator(s), organization(s) before a court of competent jurisdiction and end in a conviction. Criminals are more sophisticated, cunning, and organized thus making it more difficult for law enforcement to conduct a successful investigation.

The Department recognizes that it must collect information and process that information into a product that will meet the Departments needs in its endeavors to be proactive in the process of carrying out the Department's mandate to protect society and manage and direct the Department's resources to its best advantage in combating crime.

PROCEDURE:

1. RESPONSIBILITIES:

- A. The Detective Division Intelligence Unit is responsible for the proper administration in the collection of information and intelligence. The Detective Division Intelligence Supervisor will ensure all Departmental directives are adhered to.
- B. The Detective Division Intelligence Detective will collect, evaluate, collate, analyze, and disseminate criminal information and intelligence as directed by the Deputy Superintendent – Detective Division or designee.

2. COLLECTION OF INTELLIGENCE INFORMATION DATA

- A. The Commanding Officer – Detective Division or Intelligence Supervisor will make annual evaluations of intelligence operations to ensure new legislative and or judicial guidelines are being adhered to.
- B. Electronic surveillance will only be conducted in accordance with appropriate federal and state regulations.
- C. Photographic surveillance may be conducted only with specific authorization from an Intelligence supervisor to:
 - 1. Identify any/all individuals engaged in illegal activities.
 - 2. Identify any/all individuals as either members or associates of

criminal groups or criminal organizations.

3. Provide evidence of any illegal activity involving individuals, members of criminal groups or criminal organizations.
- D.** Photographic surveillance will be conducted in a manner that is permissible by law and one that does not constitute a violation of privacy.
- E.** All Photographic surveillance conducted by and/or submitted to the Detective Division Intelligence Unit will be reviewed by the Intelligence supervisor for approval and placement in the Intelligence files.
1. Person(s) not deemed to be reasonably suspected of involvement in a criminal activity will not be recorded or retained in Intelligence files.
 2. Photographs taken that do not meet Department policy and procedure will be immediately destroyed.
 3. If approved, the investigating officer will attach a report identifying individuals in the photograph(s).

Detective Division personnel will be properly instructed in their duties and responsibilities as it pertains to this Policy and Procedure.

Officers who feel that they possess information with tactical intelligence value shall submit such information to the Detective Division in writing.

- F.** Members of the Detective Division will evaluate the information and make a determination as to whether it possesses value as tactical intelligence. A decision will then be made whether further investigation or action is warranted at that time.
- G.** In all cases, the submitting officer will be notified of the final disposition of the information received.
- H.** All information received by Department personnel will be properly evaluated and the source of such information noted. **(See Appendix A)**
- I.** The intelligence reports prepared by members of the Department will be properly maintained in the Intelligence files. Any Department investigative report(s) that may contain information that could be utilized for intelligence purposes will be properly maintained in Department files.
- J.** Attempts should be made to obtain investigative and intelligence reports from other federal, state, county, and municipal law enforcement agencies that may be of a benefit to the Department in its endeavors to investigate subjects or organizations

suspected of being involved in criminal activity. The information will be evaluated as required by members of the Department prior to inclusion into the Department's Intelligence files.

3. REPORTING

- A.** Departmental personnel will submit investigative and intelligence data on electronic forms provided:
 - 1.** Department Intelligence System - General and sensitive intelligence data.
 - 2.** Department Incident Report - All complaints and allegations. Any complex information obtained during a lengthy investigation. Other information that is not considered intelligence information.
- B.** The contents of reports should be objective and fact finding and distinguish reliable or verified data from that of opinion, inference, or hearsay. The report should be arranged in a chronological and concise manner.
- C.** All names contained within the report will be fully identified to the fullest extent possible.
 - 1.** All personal identifiers.
 - 2.** All duplicate identifiers.
 - 3.** All aliases.
 - 4.** All criminal record number(s).
 - 5.** Any other information pertinent to the identification of the subject.
- D.** Ideally, all data contained in an intelligence report should be substantiated by other sources. If this is not possible, the officer should be reasonably assured of the validity of the data. This requirement should not be construed as a restraint, but rather as an impetus to a professional investigation.
- E.** Information obtained from an informant will be so indicated according to established Department policy.
- F.** All intelligence and investigative reports classified by Detective Division supervisors as Authorized Access Only will meet any of the following criteria:
 - 1.** The physical and economic well-being of an informant or an informant's immediate family could be jeopardized if the information was released;
 - 2.** A pending investigation could be jeopardized if the information was improperly released;
 - 3.** Any information extracted from an electronic surveillance unless authorized by law.

4. The possible physical or economic extortion of an individual if the information were improperly released;
 5. Any information of a restricted and/or confidential nature obtained from another agency.
 6. When approving a report that meets any of the above criteria, the reviewing supervisor shall request that the report be sealed within the Department's Larimore Report Writing System.
 7. This request should be sent to a supervisor from the appropriate division with access to the sealing function within the Department's Larimore Report Writing System. This supervisor will then secure the report, thereby limiting access to designated personnel.
- G.** Commanding Officer – Detective Division, Detective Supervisors, and Intelligence Detective will maintain sole custody of Authorized Access Only files and dissemination of such will be with Detective Intelligence Supervisors specific authorization. Access to Authorized Access Only files is limited to Commanding Officer – Detective Division, Detective Supervisors, and Intelligence Detective.
- H.** Intelligence and investigative reports designated as Authorized Access Only will be submitted directly to Detective Intelligence Supervisor or designee. At no time should this type of report be submitted through normal channels.

4. RECORDING OF INTELLIGENCE INFORMATION/DATA

- A.** Supervisors will review any information prior to it being recorded or stored in Departmental files for the purpose of:
1. Determining if the information meets the intent and purpose of the Department.
 2. Deleting information/data not in the best interest of the Department or law enforcement.
 3. Deleting information not in compliance with Departmental directives.
 4. Indicating a supervisor's review in the appropriate manner.
- B.** All names of individuals, corporations, and/or businesses contained in intelligence and investigative reports will be indexed in a separate master file. If the information is classified as Authorized Access Only, it will be contained in the sensitive information file accessible only to Commanding Officer – Detective Division, Intelligence Supervisor and Intelligence Detective. Reports contained within the Department's Larimore Report Writing System may also be sealed thereby limiting access to designated personnel.

- C.** All electronically indexed master files will provide the requisite data for positive identification of the individual contained therein. Sufficient information will be included in abstract form to eliminate the need to refer to other data bases.
- 1.** If investigators obtain information but lack positive identifiers, the master index file will reflect the alias known. Subsequent attempts will be made by investigators to update the data.
- D.** All intelligence information received by Department personnel will meet any of the following criteria:
- 1.** Arrest, indictment, or outstanding warrant(s). The reports should summarize the criminal history of the individual and reflect the State Identification Number (SID), Federal Bureau of Investigation (FBI) number, and/or the case identification number of the submitting source;
 - 2.** Any individual identified as a perpetrator of a crime by a witness or competent evidence;
 - 3.** Any individual who threatens violence towards people or property;
 - 4.** Any individual wherein reasonable suspicion exists to believe the individual has or is engaged in or conspiring to engage in criminal activity;
 - 5.** Any information that depicts the extent or scope of Organized Crime activity;
 - 6.** Any information relating to the identity of a victim, witness, or complainant of Organized Crime or a subject(s)' social, political, business, or professional associations where said information reasonably demonstrates to a supervisor that a potential for future criminal conduct exists;
 - 7.** Any information concerning an individual's or organization's criminal activity that provides tactical and/or strategic intelligence
 - 8.** Information required by law or directives of the department.
- E.** Photographic surveillance images will be maintained in conjunction with the intelligence report submitted. When the intelligence report is purged, all photographic images will be destroyed.
- F.** The Department's intelligence files will be audited every five years, or as required. The Department's Larimore Intelligence System will automatically send a notification indicating that it contains information which is approaching this five year period. A Detective Division supervisor will review, reevaluate, and/or purge

any data no longer meeting Departmental guidelines. Any information may be declassified as established by Departmental guidelines and/or as required by law.

- G.** The decision to purge information should be guided by the following considerations:
 - 1. The number of requests for that file/individual;
 - 2. Validity of the data;
 - 3. Reliability of the data;
 - 4. Departmental guidelines;
 - 5. Federal/state law;
 - 6. Time in the file;
 - 7. Future utility.
- H.** Intelligence information will be purged as permitted by law when it is determined:
 - 1. The data is no longer relevant or necessary for Departmental -purposes;
 - 2. The data is obsolete, and updating the information is unwise;
 - 3. The data contains no present and/or future strategic or tactical intelligence utility.
- I.** Legal counsel will be sought from the Office of Town Counsel when uncertainties arise as to the legality of intelligence information.

5. DISSEMINATION OF INTELLIGENCE DATA

- A.** Departmental personnel will treat as confidential the business and affairs of the Department. They will not impart information to anyone except to those for whom it is intended, authorized, directed by a supervisor, or as may be required by law or legal process. They will not talk for publication, nor be interviewed, nor make public speeches on law enforcement business unless specifically authorized by Chief of Police.
- B.** All requests for intelligence data will be entered into the subject's file. The entry should reflect the requesting agency and date so as to aid in coordinating investigative efforts and for auditing purposes.
- C.** Prior to dissemination of any intelligence data, a supervisor should be guided by the following considerations:

1. The accuracy and reliability of the information;
 2. Whether the release of the information would compromise the confidentiality of a source of information;
 3. Whether the release of such information could jeopardize the informant or his/her family;
 4. Whether the release of such information could jeopardize the results of an ongoing investigation;
 5. Whether the information is of a confidential or restricted nature;
 6. The requester's "NEED TO KNOW" and "RIGHT TO KNOW."
- D.** No intelligence information will be released to any Department individual or organizational entity without the specific authorization of Commanding Officer – Detective Division, or designee.
- E.** All Requests for intelligence information will be made known to Commanding Officer – Detective Division or designee. Verbal or written requests will:
1. State the reason for the request and nature of the investigation;
 2. Be appropriately recorded in the dissemination log with the necessary entries, and maintained for a period of no less than five calendar years.
- F.** Any intelligence data disseminated will contain the following statement:

The attached information is produced by the Brookline Police Department and contains sensitive material concerning law enforcement activity within the Town of Brookline. Any dissemination of the attached information that is not authorized by the Brookline Police Department is strictly prohibited and may constitute a violation of Massachusetts General Laws, c. 268A, § 23 and c. 6, §172 (the CORI statute),. Any individual, agency or organization, public or private, that receives or obtains this information without specific authorization from the Brookline Police Department, shall not collect, store, disseminate, or use such information in any manner or for any purpose. Unlawful dissemination of this information may adversely impact ongoing investigations, disclose protected witness identities, and thereby compromise law enforcement officers' safety and the safety and welfare of the public.

The substance of this message, including any attachments, may be confidential, legally privileged and/or exempt from disclosure pursuant to Massachusetts

law. It is intended solely for the addressee. If you received this in error, please contact the sender and delete the material from any computer.

- G.** Departmental intelligence and investigative report information will only be disseminated as applicable under this current policy and procedure and applicable federal or state law. Any questions will be determined by Commanding Officer – Detective Division or designee.
- H.** All intelligence information requested by an officer conducting a criminal investigation on behalf of their agency and has a right to know and a need to know will be forwarded to that officer only.
- I.** In the unlikely event a request is determined to be for non-law enforcement purposes, a Detective Intelligence supervisor will be contacted and informed immediately.
- J.** No Authorized Access Only information will be disseminated without the specific authorization of Commanding Officer – Detective Division.
- K.** Information extracted from electronic surveillance will be maintained in the Intelligence File.
 - 1. Dissemination of electronic information will be done according to applicable statute law.
 - 2. There will be no duplicate recordings without the specific authorization of District Attorney.
 - 3. If loaned to another agency, the requester will sign for said material and adhere to this Departmental or Court of Competent Jurisdictions guidelines.
- L.** Surveillance photographic images will only be disseminated with the specific authorization of Commanding Officer – Detective Division or designee and according to Departmental guidelines.

6. SOURCES OF INTELLIGENCE INFORMATION

- A.** Intelligence information can be garnered from but not limited to the following sources:
 - 1. Information obtained from reliable informants;
 - 2. Telephone tolls of an individual suspected of committing an illegal act. Such information can be subpoenaed by law enforcement personnel upon authorization of a court. Proper analysis oftentimes aids in substantiating

intelligence information.

Covert surveillance of social gatherings and events frequented by persons engaged in organized criminal activity, or reasonably suspected of criminal activity. This oftentimes provides indicators of inter and intra criminal group associations. Relationship between subjects should be identified.

- B.** The officer's report should reflect what, if any, information is obtained from secondary source(s) (motor vehicle registrations, telephone tolls, etc.), and should indicate the relationship between subjects. The officer should be reasonably certain that the secondary data on the primary subject is valid and accurate. Any such covert surveillance will be subject to the approval of a supervisor.
- C.** All intelligence information unable to meet Departmental guidelines will be submitted for analysis by a supervisor. This intelligence data will be audited every two years, or as needed.
- D.** The Brookline Police Department does not employ or condone the indiscriminate use of covert surveillance of social, political, or religious functions in the furtherance of the Department. Oftentimes these functions are attended by individuals exercising their legitimate constitutional rights. Department supervisors will ensure that the legitimate rights of individuals are not violated.

7. SECURITY OF INTELLIGENCE INFORMATION

- A.** Detective Intelligence supervisors will ensure that all information contained electronic files are secure.
- B.** Only the Detective Intelligence Unit personnel will have access to the master index file.
- C.** Detective Intelligence supervisor and Intelligence Detective will maintain custody of intelligence information classified as Authorized Access Only.
- D.** All authorized visitors, regardless of agency, are required to register with the Front Desk Officer prior to gaining admission to the intelligence file and/or records area. Those refusing, unwilling, or unable to register will be politely denied entrance.
- E.** All authorized, registered visitors will be escorted by Department personnel for the entire duration of the visit to the intelligence file and/or records area.
- F.** All Department files will be secured when not being utilized by a supervisor or designee.

8. TRAINING OF PERSONNEL [42.1.6(c)]

- A. Department personnel shall be trained in this policy upon initial employment during their Initial Training Program, and such training will be documented using the New Employee Checklist.
- B. Training should emphasize that all personnel, regardless of their assignments, have a role in criminal intelligence and the sharing of information. Training can range from information learned at roll call, department bulletins to more advanced training classes as needed.
- C. Current employees shall receive a copy of this policy and will receive training on at use, including but not limited to the following:
 - i. the responsibilities of all agency personnel
 - ii. procedures for safeguarding, securing, and storing information
 - iii. procedures for ensuring that information collected is limited to criminal conduct or relates to activities that present a potential threat to the jurisdiction;
 - iv. legal and privacy requirements
 - v. documentation, reporting, and dissemination of information and
 - vi. procedures for purging out-of-date or incorrect information

APPENDIX "A"

EVALUATION OF THE INTELLIGENCE SOURCE & INTELLIGENCE INFORMATION/ DATA

A. All sources of information will be evaluated as one of the following:

1. Reliable
 - a. Certain of the authenticity, trustworthiness, and competency.
 - b. History of complete reliability.

2. Usually Reliable
 - a. Occasional doubt of the authenticity, trustworthiness, and competency.
 - b. History of reliable information most of the time.

3. Fairly Reliable
 - a. Usually some doubt of the authenticity, trustworthiness, and competency.
 - b. History of reliable information some of the time.

4. Not Usually Reliable
 - a. Definite doubt of the authenticity, trustworthiness, and competency.
 - b. History of occasional reliability.

5. Unreliable
 - a. Almost certain of problems of authenticity, trustworthiness, and competency.
 - b. History of unreliable information.

6. Reliability Unknown
 - a. Cannot be judged.

B. All information/data will be evaluated as one of the following:

1. Confirmed as True
 - a. Confirmed by independent sources.
 - b. Logical in itself.
 - c. Agrees with other information on the subject.

2. Probably True
 - a. Not confirmed.
 - b. Logical in itself.
 - c. Agrees with other information on the subject.

3. Possibly True
 - a. Not confirmed.
 - b. Reasonably logical in itself.
 - c. Agrees somewhat with other information on the subject.

4. Doubtfully True
 - a. Not confirmed.
 - b. Not illogical in itself.
 - c. Not believed at the time of receipt of the data although possible.

5. Improbable
 - a. Feasibility questioned.
 - b. Is illogical in itself.
 - c. Contradicted by other information on the subject.

6. Cannot be Judged

C. Attempts should be made to substantiate the information through other sources.