





## **POLICIES AND PROCEDURES MANUAL**

	<b>COLLECTION AND PRESERVATION OF EVIDENCE</b>	
	<b>POLICY NUMBER: 83-1</b>	ISSUING AUTHORITY 
	<b>EFFECTIVE DATE: June 12, 2025</b>	Christine A. Elow Police Commissioner

### **I. GENERAL CONSIDERATIONS AND GUIDELINES**

The effective investigation of crime and prosecution of offenders requires that information is obtained through the application of scientific knowledge and methods. The proper identification, collection, and preservation of physical evidence, as well as its prompt submission to the lab, are essential functions of the police department. In the process of collecting and preserving evidence, the health and safety of all present at the scene should be the primary consideration.

### **II. POLICY**

It is the policy of the Cambridge Police Department to:

- A. identify, collect, and receive all evidentiary property in accordance with strict guidelines to preserve their identity, integrity, condition, and security while in the custody of the department;
- B. protect all evidence against loss, contamination, and deterioration; and
- C. exclude the processing of evidence that Crime Scene Services personnel believe to be contaminated, improperly handled, or has little or no forensic value.

### **III. DEFINITIONS**

- A. *Amanda's Law*: M.G.L. c. 271, § 51, also known as *An Act Relative to Taking or Transmitting Images of Crime Victims by First Responders*. This statute makes it a criminal offense for first responders, including police officers, to take or disseminate pictures of victims of crimes, crashes, or emergencies unless the pictures are taken or disseminated as part of the first responder's official duties or with the consent of the victim.
- B. *Biological Evidence*: Evidence in the form of blood and other bodily fluids such as semen, spittle, vaginal secretions, and any other DNA source such as bone or tissue.

- C. *Chain of Custody*: The chronological documentation showing the seizure, custody, control, transfer, and disposition of physical and electronic evidence.
- D. *CIS*: Criminal Investigations Section.
- E. *Crime Scene*: The location where an offense has been committed and forensic evidence may be gathered.
- F. *CSS*: Crime Scene Services.
- G. *Exemplars*: The prints of an individual, associated with a known or claimed identity, and deliberately recorded electronically, by ink, or by another medium such as *known prints*.
- H. *Fingerprint*: An impression of the friction ridges of all or any part of the finger.
- I. *Latent Print*: Generic term for unintentionally deposited friction ridge detail; also refers to a friction ridge impression of unknown origin that is not readily visible.
- J. *LPE*: Latent Print Examiner.
- K. *Palmprint*: An impression of all or any part of the palmar surface of the hand.
- L. *PSIT*: Public Safety Information Technology.
- M. *Tenprint*: A controlled recording of an individual's available fingers using ink, electronic imaging, or other medium.
- N. *Trace evidence*: Physical evidence so small, in size or forensic detail, that an examination requires a stereomicroscope, a polarized light microscope, or both. Trace evidence generally includes hairs, fibers, glass, paints, and soil.

## IV. PROCEDURES

- A. 83.1.1 (M) 24-Hour Availability
  - 1. A Crime Scene Technician and/or detective can be called to respond to the scene of a crime where forensic evidence may be present at any time of day or night.
    - a. Detectives are trained by Crime Scene Services Technicians in basic crime scene response, evidence processing, and evidence collection to a level that satisfies Crime Scene Services standards.
    - b. When department Crime Scene Technicians or detectives are not available, the Massachusetts State Police (MSP) should be called to respond.
- B. 83.2.1 (M) Guidelines and Procedures Used for Collecting, Processing, and Preserving Physical Evidence in the Field
  - 1. First responder responsibilities and precautions include the following.
    - a. Secure the scene and provide for the safety of officers, victims, witnesses, and suspects.

- b. Provide first aid, call for an ambulance if necessary, and call for a supervisor to respond.
  - c. Establish a perimeter.
  - d. Establish a crime scene log and call for a supervisor.
  - e. Identify and mark evidence in plain view.
- 2. The collection, storage, and transportation of evidence shall provide for the identification, integrity, preservation, and security of all items believed to have forensic value.
  - a. Personnel conducting these tasks shall use gloves and packaging materials designed for the purpose, absent exigent circumstances.
  - b. Personnel assigned to transport evidence shall take all necessary precautions to protect against loss, contamination, and deterioration.
  - c. All sworn officers should submit evidence and latent prints to Crime Scene Services through the Property and Evidence Unit or through the temporary storage lockers. Officers shall include a Property Submission Form along with the property or evidence.
  - d. Crime Scene Services personnel may collect evidence and/or latent prints from the field and secure them in the CSS laboratory directly, without needing to submit that evidence through the Property and Evidence Unit.
  - e. Crime Scene Services may accept evidence and/or latent prints from sworn personnel of an external agency with the approval of a CIS Lieutenant.
- 3. All sworn officers in the department shall receive basic evidence collection training in the police academy. Further training will be provided during field training, and on-going periodic training during in-service. CSS personnel may distribute training bulletins as needed.
  - a. Crime Scene Services Technicians should receive advanced training and attend periodic additional training as needed.
- 4. Procedures for transfer of custody of physical evidence are as follows.
  - a. If CSS personnel are collecting evidence in the field and will have continuous control of an item until it is secured in the CSS laboratory, it shall be placed in an evidence container for transport. It is not necessary for the package to be sealed and dated at the time of collection.
  - b. Once processed, the item will be transferred to the Property and Evidence Unit for secure storage by way of the evidence lockers.
  - c. Any additional transfer, such as to a lab, shall be documented in the department Automated Records Management System.
  - d. The record of transfer of physical evidence shall include the date and time of transfer, receiving person's name, reason for the transfer, name and location of the laboratory, and examinations requested.

- e. Evidence requiring information to be submitted to national databases shall be done by the following individuals in a timely manner.
    - (1) All officers shall submit evidence to the Property Unit prior to the end of shift unless a delay is authorized by a supervisor and then as soon as practical thereafter.
    - (2) After the completion of all necessary processing procedures, CSS shall notify the Property Unit of the transfer of such evidence as soon as possible for prompt transfer and submission to national databases.
  - f. A clear, well-documented electronic chain of custody record shall be maintained in the Automated Records Management System from the time an item of evidence is collected or received until the point at which that item is released.
    - (1) These records shall identify which specific person or unit took possession of each evidentiary item and/or where each item is located at each point in time between receipt and release.
    - (2) The chain of custody records, in addition to each evidence-packaging container, should contain the results of fingerprint processing attempts, stating if the item tested was positive or negative for the presence of latent fingerprints.
- C. 83.2.2 (M) Photography, Video, and Audio Evidence
- 1. Procedures pursuant to the collection and preservation of evidence include the following.
    - a. Procedures for conventional and digital photography.
      - (1) Department detectives are assigned digital cameras; all patrol supervisors have access to digital cameras; and some patrol vehicles, such as the report cars, are also equipped with digital cameras.
      - (2) Patrol officers at a scene may use their personal cell phones to document the scene and shall follow department protocol for sending the images, video, or audio to their department email addresses. Officers should delete all related material from their cell phones and computers once uploaded to the ARMS.
      - (3) Media evidence collected by department personnel should be submitted on a SD card or uploaded to the incident report in the ARMS.
      - (4) Booking videos are maintained by the PSIT Unit. When a request for video footage from booking is submitted to the Property and Evidence Unit by the courts or the District Attorney's Office, the request is forwarded to PSIT. PSIT will send the footage to the Property and Evidence Unit as an uploaded file in the ARMS. That data file is then transferred to either a thumb drive or CD which is transported by vehicle or mailed to the requestor. CIS personnel may also utilize *NICE Investigate*.
      - (5) Booking photos are stored in the ARMS with access limited to authorized personnel.

- b. Audio interviews are recorded on a CD and submitted to the Property and Evidence Unit. Officers may audio record on a personal device if necessary and submit the recording to the Property and Evidence Unit via email or other storage device. An officer may upload an audio recording directly to the ARMS.
- c. Procedures for imaging and video are as follows.
  - (1) *Case Cracker* is a video and audio recording program used in interview rooms. All interviews are recorded using this program on a computer that is maintained in the Criminal Investigations Section.
  - (2) Access to the computer is limited to authorized personnel only and users must log in with a secure login and password.
  - (3) Detectives can create a DVD of the recording, which can be submitted to the District Attorney's Office. CIS personnel may also utilize *NICE Investigate*.
  - (4) Surveillance video that has been captured by an outside private entity may be requested and received by the department to aid in the investigation of a case, including motor vehicle crashes and criminal activity.
- d. Procedures for the use of personally owned devices are as follows.
  - (1) The department allows police officers on scene to use personal cell phones to document the scene.
  - (2) These images/videos should be transferred to the officer's department email as soon as possible and once delivery to the email address is confirmed, the images/videos shall be deleted from the officer's device.
  - (3) Officers should protect the privacy and confidentiality of all persons.
- e. Amanda's Law
  - (1) Officers shall not take a photographic or digital image of a victim of a crime, crash, or emergency unless the officer takes the photographic or digital image: (1) in the performance of their official duties; or (2) upon the consent of the victim or, if the victim is unable to consent, an immediate family member of the victim.
  - (2) Other than in the performance of their official duties, officers shall not transmit, disseminate, or otherwise make available to a third person a photographic or digital image of a victim of crime, crash, or emergency without the consent of the victim, or if the victim is unable to consent, an immediate family member of the victim.
  - (3) This law does not apply to the use of body-worn cameras or cameras mounted on a police cruiser.

#### D. 83.2.3 (M) Fingerprinting

- 1. Although department detectives receive training on the processing of crime scenes for evidence and latent print collection, the CIS supervisors may choose to utilize CSS personnel

to analyze latent print evidence on-scene and assist in print collection. Any evidence should be documented thoroughly with notes, sketches, and/or photographs prior to deploying processing techniques.

- a. If latent prints are developed, the areas of ridge detail shall be identified with a latent designator, photographed, and their location described in the notes.
  - b. If collected using a lifter or cast, the lifter or cast shall be properly labeled and securely transferred to CSS to begin the analysis phase. This transfer may be done by CSS personnel, who then assume the responsibility for beginning the chain of custody record for the item.
  - c. If a lift or cast is attempted, and the lift does not contain any ridge detail, the lift or cast may be discarded.
2. It may be necessary to collect fingerprint exemplars from individuals with known connections to the scene and/or evidence being processed for fingerprint development, such as victims or witnesses. These records are referred to as elimination prints. Elimination prints may be collected on-scene by department detectives or CSS personnel. Additionally, individuals may come to Robert W. Healy Public Safety Facility where CSS personnel or detectives can collect the exemplars. Elimination prints should contain multiple pieces of information including:
  - a. the name of donor;
  - b. the donor DOB and signature;
  - c. the case number;
  - d. examiner's signature; and
  - e. fingerprint card identifying number, EP1 or EP2 for example.
3. Elimination prints shall not be used for any purpose other than fingerprint comparisons for the specific case for which they were collected. Elimination print cards shall be entered into the chain of custody under the appropriate case number and stored in the CSS case file.
4. Evidence submitted to Crime Scene Services for latent print processing varies depending on the surface type. The Crime Scene Services Procedural Manual outlines the appropriate reagents and application procedures used by CSS to recover friction ridge detail and to ensure the methods are valid.
5. Latent print processing methods used by CSS have been validated and are considered acceptable within the field.
6. The following describes the step-by-step procedures for processing various pieces of evidence based on their surface type.
  - a. In the event an examiner encounters an unfamiliar surface type that they have not had experience in processing, the examiner shall determine the best suitable processing

- method. The examiner must perform the processing method on a simulated piece of evidence prior to the actual evidence.
- b. Analytical procedures for surface types not already included in the manual may be added. Information gathered from scientific journals or in-house research on the procedure shall be validated prior to using the new method or chemical on evidence submitted for latent print processing.
  - c. Any new technique tested and validated in-house shall follow the *Validation of New Techniques* section in the Crime Scene Services Quality Manual.
  - d. Quality control measures used to determine the effectiveness of each reagent, such as ninhydrin, have been included in CSS Procedural Manual. No quality measures have been specified for reagents that do not require this testing, such as fingerprint powder.
  - e. Safety concerns, processing conditions, and application guidelines are included for each reagent used in the processing of evidence.
  - f. The temperature and humidity conditions of the laboratory shall be monitored and recorded on a weekly basis on the temperature and humidity log. The temperature should fall between 60-75°F and a humidity level between 30-60%.
7. Latent print examiners shall examine and perform an analysis using the appropriate ACE-V methodology on all latent prints that are submitted to CSS. At the examiner's discretion, based on information gathered in the analysis process, prints determined to contain friction ridge detail of sufficient quality and quantity (SRD) may be entered into the AFIS system.
- a. Latent prints entered should contain identifying case information including case number, crime type, name of who entered the latent, and the date of latent entry.
  - b. A Latent Print Examination Worksheet shall be completed for each latent print that is analyzed. The *AFIS Entry* section of this worksheet shall be completed for each latent print that is entered into the AFIS system.
  - c. Once a suspect has been identified via latent prints (AFIS or manual comparison), it is at the discretion of the examiner to enter other case latent prints into AFIS. It is not required that all latent prints for a case be entered into AFIS, following a suspect/victim identification.
  - d. The worksheet(s) shall then be retained in the case file. AFIS entries shall also be noted in the Latent Print Examination Report completed by the assigned LPE.
8. As a result of entering new latent records, candidate lists containing possible identifications are generated. These candidate lists developed from the entry of new latent searches shall be reviewed by a qualified examiner in a timely fashion.
- a. If there is a potential match on the candidate list, it shall be examined according to the ACE-V section of the CSS Procedural Manual and documented on the Latent Print Examination Worksheet. When making an identification, the LPE shall retrieve the entire

exemplar record and request additional exemplars if needed to perform a proper analysis. Identifications should not be made based on what is seen on the AFIS screen alone.

- b. All AFIS systems are treated merely as a search tool, and all conclusions shall come at the determination of a qualified LPE.

- (1) Regardless of the system-generated score, comparisons shall be conducted on every record in the candidate list.

- (2) Candidate lists for each latent print shall be stored in the CSS electronic case file.

E. 83.2.4 (M) Equipment and Supplies

- 1. Crime Scene Services has access to personnel, equipment, a fully stocked vehicle, and supplies used for processing scenes including:
  - a. recovery of latent fingerprints;
  - b. photography and videography;
  - c. sketch of the scene; and
  - d. collection and preservation of physical evidence.
- 2. All such equipment and supplies shall be maintained in a ready condition for immediate deployment when necessary.

F. 83.2.5 (M) Procedures, Seizure of Electronic Equipment

- 1. The following guidelines establish procedures for the seizure and storage of computers, digital storage media, cellular devices, digital cameras, digital camcorders, and other electronic devices capable of storing digital information, and for the preservation and storage of digital evidence.
- 2. All evidence seized and/or processed pursuant to this policy shall be conducted in compliance with all state and federal laws, and policies/ordinances of the City of Cambridge and the Cambridge Police Department.
- 3. When seizing a computer and other accessories, officers should perform the following to the best of their ability at the time of the seizure.
  - a. Verify that the scene is safe and free of any hazards.
  - b. Utilize PPE including gloves so that any potential fingerprints or biological/trace evidence is not disturbed.
  - c. Refrain from reviewing, accessing, or opening digital files.
  - d. Photograph each item, including cable connections to other items.
    - (1) If easily available, photograph the serial numbers and identifying information for the device.
  - e. Photograph the screen of each device that is to be seized.



- f. If the device is powered off, do not turn it on.
  - g. If the device is powered on, it is essential to leave it turned on, if possible.
    - (1) Contact a member of the Cyber/Electronics Crime Unit or the US Secret Service Electronic Crimes Task Force for assistance in the application of forensic tools.
  - h. Make a log of all devices that the officer will be seizing and label each item with the case number and an item number, such as a letter.
  - i. To maintain the integrity of the evidence, take care in the handling and transporting of the computer and any digital storage media, such as USB drives, external hard drives, CD/DVDs, and memory cards.
  - j. Log all items into the Property and Evidence Unit in accordance with department policy.
  - k. If the case involves potential child pornography, these items need to be stored within the Cyber/Electronic Crimes Unit. Log the evidence on an Evidence Submission Form. Submit the form into the Property and Evidence Unit, and all devices to a member of the Cyber/Electronic Crimes Unit.
  - l. Officers should then document the seizure of the evidence in a report. The report should contain the following.
    - (1) Identifying information about the device.
    - (2) Where the device was located and whether it was powered on.
    - (3) Who was using the device at the time.
    - (4) Who claimed ownership of the device.
    - (5) The main purpose of the device.
  - m. When seizing a device, if the power cord is available, seize the power cord, as some manufacturer's cords are proprietary.
4. The following guidelines relate to cellular devices connected to any cellular network or wi-fi connection.
- a. Officers should use PPE and not attempt to access, review, or search the contents of the device prior to examination by a trained investigator. By accessing the device, an officer risks manipulating data on the device.
  - b. Photograph the device and the screen.
  - c. If officers have decided to seize a cellular device, they should remove the device from cellular networks. Newer technology requires a device to maintain power and be turned on to successfully extract data from the device, using approved tools. To remove the device from the network, an officer should perform one of the following.
    - (1) Place the device into airplane mode, and confirm that the cellular, wi-fi, and blue tooth connections are off.

- (2) If unable to place the device into airplane mode, remove the SIM card and tape it to the back of the device.
    - (3) If available, seize the power cord.
    - (4) If possible, obtain any pass codes or pattern locks from the owner of the device.
  - d. Document any actions taken to remove the device from the network.
  - e. If the device is powered on, submit a Property and Evidence Form to the Property and Evidence Unit, and turn the device over to a member of the Cyber/Electronic Crimes Unit to place into the Cyber/Electronic Crimes Unit secure storage to charge.
  5. Officers responding to incidents involving the investigation into child pornography in which evidence is to be seized, should not upload images/videos to the ARMS or *NICE Investigate*.
    - a. All of these files will be maintained offline in the Cyber/Electronic Crimes Unit.
    - b. Officers should never have any type of image/video depicting child pornography sent to them via email, text, or by any other means.
- G. 83.2.6 (M) Report Preparation
1. The employee who processes a crime/traffic collision scene shall prepare and write the report.
  2. A detailed report shall be included in every case file for all cases involving evidence processing. The report may include but not be limited to the following information.
    - a. General incident information such as the case number and a description of the incident; names of victims, witnesses, suspects if known; and any action taken by first responders.
    - b. The name of the Crime Scene Technician or Crash Investigator assigned to the case, including the date and time of arrival at the scene.
    - c. The date and time of the processing and/or investigation if different from the date and time of arrival.
    - d. A record of the designated number assigned to each item of evidence.
    - e. A description of each item's packaging and processing results, including a list of any latent prints, DNA samples collected, measurements taken, and photographs.
    - f. The processing methods used.
- H. 83.3.1 (M) Collecting from Known Source
1. In some cases, materials and substances should be collected from a known source, whenever available, for submission to the laboratory for comparison with physical evidence collected.
  2. Paint chips, broken glass, and wood splinters collected as evidence are usually associated with more serious cases that are assigned for investigation to the Mass State Police. Very rarely

will a Cambridge Police Department Crime Scene Technician collect samples from a known source. In such cases, the Technician may call and consult with the Mass State Police.

I. 83.3.2 (M) Evidence, Laboratory Submission

1. Procedures for submitting evidence to an accredited forensic laboratory are as follows.
  - a. All evidence that is submitted to an outside lab will be sent from the Property and Evidence Unit by the Property Clerks who are the persons ultimately responsible for the submission. This includes all forms of evidence, such as wet and dry blood, sexual assault kits, biological evidence, drugs, guns, and bulk items.
  - b. Evidence is usually transported in the original secure packaging, dated, sealed, and initialed by the processing authority. The name or initials on the submission will be the last person handling the evidence.
  - c. The MSP is the primary entity used for processing all evidence requiring a laboratory. The MSP has its own forms that must be submitted with the evidence.
  - d. The chain of custody is part of the form used for all submissions to the lab. The Cambridge Police Department will follow all directives and requirements of the MSP for lab submissions.
  - e. All laboratory results shall be returned to the Cambridge Police Department in writing.