Cambridge Police Department	**POLICY & PROCEDURES**	**No. 412**
	Subject/Title: **Mobile Data Terminals & Handheld Devices**	
	Issuing Authority: Robert C. Haas, Police Commissioner	**Review Date:** May 10, 2010 **Issue Date:** August 5, 2010 **Effective Date:** **Rescinds:**
References/ Attachments:	**Accreditation Standards:** 41.3.7	

I. PURPOSE:

The purpose of this policy is to provide police officers with guidelines for the proper use of Mobile Data Terminals (MDT's) and handheld mobile computers. To ensure legal and proper use of this resource, all department members must have a thorough understanding of the content of this policy and the importance of it. In addition, it provides operational procedures for the proper access, use, and security of the information that can be obtained from mobile systems and handheld devices.

II. POLICY:[1]

It is the policy of this department that:

- Employees using mobile computers and software will be trained to the appropriate level of use;
- Mobile computers are to be used for legitimate police business only;
- Mobile Data Computers (MDT) will be used in a manner that it does not pose a hazard while operating the cruiser;
- Employees are responsible for ensuring that mobile computers are used in an effective, efficient, and lawful manner; and

[1] CALEA Std.: **41.3.7** – *If the agency has computerized mobile data access capabilities or other similar technologies, a written directive establishes procedures for its use, to include:*

a. *The unauthorized introduction of software programs or other files; or*
b. *The manipulation or alteration of current software running on agency-owned mobile, desktop or handheld computers.*

- Random and periodic audits of MDT use and log files will be made at the department's discretion, and compliance with guidelines wert forth by the FBI and the Criminal History Systems Board (CHSB).

III. GENERAL CONSIDERATIONS AND GUIDELINES:

The advent of computer access to the Criminal Justice Information System (CJIS) and the department's Records Management System (RMS) from police vehicles and hand-held computers has put a powerful tool into the hands of police officers. Access to CJIS and the gateway to the national files are controlled by the Criminal History Systems Board (CHSB), under an agreement with the FBI CJIS Division.

CHSB is also charged with the maintaining network and user security. Software vendors who apply to CHSB for access to CJIS files must pass rigorous reliability and security testing prior to being certified for use in Massachusetts.

All CJIS applications must maintain transaction log files. Some portions of log files of data queries and mobile-to-mobile communications are a public record and may have to be released pursuant to a public records request. There is no reasonable expectation of privacy in the queries and messages you send and receive using these systems and programs.

Given the complexity of these systems and their vulnerability to outside interferences, it is imperative that officers strictly adhere to the guidelines set forth within this directive.

IV. DEFINITIONS:

A. **Mobile Data Terminal (MDT):** A cruiser-mounted or otherwise portable computer used by trained and certified department members for purposes of accessing CJIS, CHSB, LEAPS records, police department Records Management System, or other available information via secure access to various information bureaus.

B. **Accounts:** All users are responsible for the proper use of the accounts, including proper password protection. Accounts will be created and assigned by the department's IT Administrator.

C. **Criminal Justice Information System (CJIS):** The computerized network, services and applications that offers law enforcement agencies within the state

and nationally secure access to state and interstate criminal history, driver and vehicle records, restraining orders, and other important confidential data.

D. Criminal History Systems Board (CHSB): The state agency responsible for maintaining the state's law enforcement data communications network and systems and for the processing and dissemination of C.O.R.I. to authorized entities and persons.

E. Criminal Offender Record Information (C.O.R.I.): C.O.R.I. system is the 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 or 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's policy entitled, ***#360 – Criminal Justice Information System.***

V. PROCEDURES:

A. Hardware Devices: For purposes of this directive, hardware devices refer to the laptop computer or handheld device, and the peripheral devices associated with this equipment.

1. Some desktop, static computers within the police station may also be connected to the mobile network, Such systems may include:

   a. Dispatch workstations;

   b. Supervisory and administrative workstations; and

   c. Clerical workstations.

2. Computer connectivity to the mobile system may be accomplished by a vehicle mounted modem.

3. Servers which run mobile applications shall be located in a secure facility with access limited to authorized persons only.

B. Software Applications: For purposes of this directive, software applications refer to the programs and applications that are used to operate the various systems that are accessible through the mobile data terminals or handheld devices.

1. Mobile software applications running on the mobile network are:
   a. CJIS – Access through to the CJIS network is through the department's mobile data software system.

   b. Dispatch – The department's CAD and RMS are controlled by Q.E.D. software.

2. Only authorized software may be installed and operated on the department's MDT or handheld devices. Unauthorized software programs or files may not be introduced into the agency computers.[2]

3. Authorized software may not be manipulated or altered on any agency-owned mobile, desktop, or handheld computers. Modifying computer settings, such as changing Windows and other associated software applications is prohibited.

C. User Access: Each authorized user of the system will be issued a login name and password. Users are responsible for maintaining the security of their passwords, and should never share them with anyone, including other employees.

1. Further, employees authorized to query Board of Probation (BOP) checks must have a user name and password and be trained to at least the "Admin and Inquiry" level of use.

2. Each member of the department who has been authorized to access the CJIS network will be issued a username and password by the department's IT Administrator.

D. Use of Mobile Data Terminals: As part of the initiation procedures for access the software applications on the MDT's, officers will adhere to the following set of procedures:

1. At the beginning of the shift, officers will check the MDT while completing their routine vehicle checks. Damaged equipment must be reported to the supervisor immediately.

2. Employees shall log into the assigned MDT and shall remain active in the system for their entire tour. If any problems are encountered, employees should check the equipment as explained in this policy under "trouble shooting" prior to reporting the equipment inoperative. Unresolved issues should be reported to the IT Unit to be corrected.

[2] CALEA Std.: **41.3.7**

3. All mobile computing transactions must conform to FCC guidelines regarding radio transmissions and shall not contain improper language or subject matter.
4. Car to car chat shall be limited to communication which is relevant to police activity.

5. All MV stops, field interviews, etc. shall be radioed into dispatch to ensure officer safety.

6. Some MDT's programs are equipped with an audible alarm so that officers are notified of pertinent messages or announcements. The audible alarm setting on all terminals shall be left on. No officer shall mute, turn off or disable the alarm(s).

7. Officers who obtain actionable CJIS information through the MDT such as a "HIT" (warrant, revoked license or registration) must have the query run through the Emergency Communications Center (ECC) to obtain a paper copy of the "HIT" and to confirm accuracy.

8. The MDT is not be used by an officer while operating a vehicle in traffic, or while the vehicle is in motion, as this may divert the officer's attention from the safe operation of the vehicle. Such queries should be run through ECC.

9. The MDT shall not be used to access or attempt to access the Internet, unless it is used in connection with the officer's official duties. Any personal utilization of the Internet through the MDT is prohibited (also refer to the City of Cambridge's ***"Internet and On-line Computer Services Use Policy"*** and the department's policy entitled, ***#212 – Internet, Email, & Computer Services*** as it relates to the permitted use of the Internet).

10. No food, beverage or any other substance that may inflict damage will be placed on or near the MDT.

11. Only the provided stylus pen or a clean finger may be used to operate the touch screen. Use of any other object to activate the touch screen is prohibited, as it may scratch or otherwise damage the screen display.

12. Laptop screens should be cleaned with a soft, clean cloth, such as a micro-fiber cloth. Use of cleaning solvents and liquid-based products on the computer is prohibited, as they often cause hazing or damage to the screen. If further cleaning is required, notify the IT Unit.

13. To ensure that officers' accounts are not accessed, officers must log off of the MDT at the end of their tours of duty and turn off the computer.

E. **Security:** Officers are expected to adhere to the security measures that are outlined as follows:

1. Vehicle Mounted MDT's:

   a. All cruises equipped with MDT's shall be locked whenever unoccupied.

   b. MDT's should be removed from any vehicle which is anticipated to be out of service for any prolonged period of time, or when the vehicle is being sent out for service through an outside service.

   c. If an MDT computer, modem or air card is discovered to be damaged or lost/ stolen; this shall be reported immediately to a supervisor, who shall take the necessary steps to render access of the device to the network inaccessible.

2. Handheld devices shall be stored in the designated chargers when not in use.

   a. If a handheld device is discovered to be lost or stolen, the loss or theft must be reported immediately to a supervisor, who will take the necessary steps to render access to data through the device inactive.

3. Any user who finds a potential lapse in security on any system shall be obligated to report the potential lapse to the IT Unit forthwith. The system(s) shall then be taken out of service until the problem can be investigated.

4. Security incidents which violate confidentiality, integrity, or availability of data must be reported to the CHSB.[3]

5. No employee shall log into any computer or application using the username and password of another employee. This action is a crime under Massachusetts General Laws and a serious breach of security.[4]

6. Care should be taken to keep information out of the view of the general public by turning the screen away or closing the laptop cover. The MDT lid shall be closed at all times when away from the vehicle.

F. **Training:** All employees using MDT's or mobile computers shall be trained on the use of the computer and software applications they are to use. CJIS users are required to be trained, tested, and certified, at the minimum, to the "Admin and Query" level of use.[5]

[3] Appendix D, CJIS Users Agreement
[4] M.G.L. c. 266, § 120F
[5] CJIS User Agreement, 3.18

G. **Data Log Files:** A transaction log of CJIS queries and responses must be maintained pursuant to 3.8.1 of the CJIS User Agreement. Files must be maintained for at least two years and must be available to CHSB upon their request. Mobile communications, data queries, and car to car chat functions are logged by the mobile software. These communications and logs may be public records and may have to be released upon receipt of a public records request.

H. **Trouble Shooting:** Some of the most common problems encountered when attempting to obtain access through the MDT, can be remedied by the checking the following steps. Prior to calling for technical assistance from the IT Unit, the user should first go through the following sequence (also refer to the attached ***Reference Guide***):

1. Computer won't power on: Check for battery light and power to the system. Lack of power may be caused by a poor connection with the connection socket or a blown fuse.

2. Computer is on, but the screen is frozen: Check to see if the mouse or keyboard is working. If so, reboot he computer. If not, shut the computer off using the power switch, wait at least ten seconds, and then turn the computer on.

3. Computer comes on and the programs load, but the user cannot log in: Ensure that the "cap lock" key is not on and that the keyboard and mouse are working. Check to see if the computer is connected to the network.

4. The computer is connected to the network:

    a. Check to ensure that the data cable is properly connected and the connector screws are tight.

    b. If the computer is equipped with a modem, check the modem to make sure that it is getting power and the data cable to make sure that is properly connected and the connector screws are tight.

    c. If the computer is equipped with an air card, check to ensure that the card is properly seated and that the antenna connection is tight.

5. The program is running, but the user does not get any CJIS data back:

    a. Check with other officers to see if they are having difficulty connecting as well.

b. Multiple vehicle programs that are inoperable may indicate a network or server issue.