	MEDFIELD POLICE DEPARTMENT	**POLICY NO. 4.09**

USE OF MOBILE DATA TERMINALS

MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **41.3.7**	DATE OF ISSUE: 06/25/2023 EFFECTIVE DATE: 06/25/2023 REVISION DATE: 11/04/2025
ISSUING AUTHORITY: Michelle Guerette Chief of Police	

I. GENERAL CONSIDERATIONS AND GUIDELINES

The advent of computer access to CJIS and department records from police vehicles and hand-held computers has put a powerful tool into the hands of police employees. Access to CJIS and the gateway to national files is controlled by the CHSB, under an agreement with the FBI CJIS Division.

Through this agreement, CHSB is mandated with providing 24/7 access to national criminal justice information files such as missing and wanted persons, Interstate Identification Index (III), convicted sex offenders, and others.

CHSB is also charged with 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.

The purpose of this policy is to provide law enforcement officers with guidelines for the proper use of Mobile Data Terminals (MDTs) and handheld mobile computers. In

order 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.

II. POLICY

It is the policy of this department that:

1. Employees using mobile computers and software will be trained to the appropriate level of use;
2. Mobile computers are to be used for legitimate police business only;
3. Employees are responsible for ensuring that mobile computers are used in an effective, efficient and lawful manner; and,
4. Random and periodic audits of MDT use and log files will be made at the department's discretion.

III. DEFINITIONS

A. MDT - Mobile Data Terminal: A cruiser-mounted or otherwise portable computer used by trained and certified department members for purposes of accessing CJIS, CHSB, LEAPS records, police department information systems 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 Account Administrator.

C. CJIS - Criminal Justice Information System: 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. CHSB - Criminal History Systems Board: 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. C.O.R.I.: “Criminal offender record information”: 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 of 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 policy on C.O.R.I.

IV. PROCEDURES

A. Hardware

1. COMPUTERS CONNECTED TO MOBILE APPLICATION SOFTWARE WILL GENERALLY BE MOBILE (LAP TOP) COMPUTERS AND HANDHELD DEVICES.
2. SOME DESKTOP, STATIC COMPUTERS WITHIN THE POLICE FACILITY, MAY ALSO BE CONNECTED TO THE MOBILE NETWORK. SUCH SYSTEMS MAY INCLUDE:
   a. Dispatch workstations;
   b. Supervisory and administrative work stations; and
   c. Clerical work stations.
3. COMPUTER CONNECTIVITY TO THE MOBILE SYSTEM MAY BE ACCOMPLISHED BY:
   a. A vehicle mounted modem;
   b. Laptop air card; or
   c. LAN.
4. SERVERS WHICH RUN MOBILE APPLICATIONS SHALL BE LOCATED IN A SECURE FACILITY WITH ACCESS LIMITED TO AUTHORIZED PERSONS ONLY.

B. Software

1. AUTHORIZED SOFTWARE
   a. Mobile software applications running on the mobile network are:
      1) CJIS –IMC;
      2) Dispatch –IMC;
      3) Chat – IMC LAN
      4) GPS – None
2. PROHIBITED [41.3.7]
   a. Only authorized software may be run on mobile computers. Unauthorized software programs or files may not be introduced into agency computers. For further information, see the department policy on Computers and Data Security.
   b. Authorized software may not be manipulated or altered on any agency-owned mobile, desktop or handheld computers. Modifying computer settings, such as but not limited to changing Windows is prohibited.

C. User Access

1. 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. For further information see the department policy on Computers and Data Security.
2. 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. A user name and password may be obtained from the CJIS Representative.

D. Use

1. At the beginning of the shift, employees shall check the MDT while completing their routine vehicle checks. Damaged equipment shall be reported to a supervisor immediately.
2. Employees shall log onto the assigned MDT and shall remain active on 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 a Department Information Technology (IT) officer to be corrected.
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 communications to obtain a paper copy of the “HIT” and to confirm accuracy.
8. It is discouraged for the MDT to be used by an officer while operating a vehicle while the vehicle is in motion, as this may divert the officer’s attention from the safe operation of the vehicle. Such queries, when practicable, should be run through communications.
9. The MDT shall not be used to access or attempt to access the internet.

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

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

E. Security

1. Vehicle Mounted MDTs:
   a. All cruisers equipped with MDTs shall be locked whenever unoccupied.
   b. MDTs should be removed from any vehicle which is anticipated to be out of service for more than five days.
   c. MDTs should be rendered non-functional when a vehicle is sent to be repaired by a non-municipal repair facility. MDTs may remain in the vehicle when the vehicle is serviced by municipal employees or by approved repair facilities.
      1) In long-term out of service situations, computers should be removed from the vehicle.
      2) MDTs equipped with air cards may have the air cards removed.
      3) MDTs which access the network through a modem should have the modem shutdown.
   d. If an MDT computer, modem or air card is discovered to be lost or 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. Any user who finds a potential lapse in security on any system shall be obligated to report the potential lapse to IT Supervisor forthwith. The system(s) shall then be taken out of service until the problem can be investigated.
3. Security incidents which violate confidentiality, integrity, or availability of data must be reported to the CHSB.[1]
4. No employee shall log into any computer or application using the username and password of another employee. This action is a crime under M.G.L. c. 266, §120F and a serious breach of security.[2]

F. Training

1. All employees using MDTs or mobile computers shall be trained on the use of the computer and software applications they are to use.

[1] Appendix D, CJIS Users Agreement.

[2] M.G.L. c. 266, §120F.

2. CJIS users are required to be trained, tested, and certified, at the minimum, to the "Admin and Query" level of use.[3]

G. Data Log Files

1. 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. For further information, see the department policy on Computers and Data Security.
2. 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:

1. Computer won't power on:
   a. Check for battery light and power to the system. Lack of power may be caused by a poor connection with a cigarette lighter plug or a blown fuse.
2. Computer is on but the screen is frozen:
   a. Check to see if the mouse or keyboard is working. If so, reboot the 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:
   a. Ensure that the "cap lock" key is not on and that the keyboard and mouse are working.
   b. Check to see if the computer is connected to the network
4. The computer is not 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. Check to ensure that the antenna cable connector is 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 as well.

[3] CJIS User Agreement, 3.18.

b. Multiple vehicle problems indicate a network or server issue.

I. Hosting Other Agencies

1. A memorandum of understanding (MOU) is required between this department and user agencies pursuant to 3.13 of the CJIS User Agreement. The agreement must be between the agency heads and must outline:
   a. Services to be provided; and
   b. Responsibilities of each party involved.
2. The agreement must be forwarded to CJIS within fourteen (14) days of execution.