



Town of Lexington

Police Department

Subject: Laptop Computer Usage	
REFERENCED: 41.3.7	
Effective Date: 09-01-2011	Review Date: Annually
By Order of: Mark J. Corr, Chief of Police	

Policy & Procedure

82C

The Municipal Police Institute, Inc. (MPI) is a private, nonprofit charitable affiliate of the Massachusetts Chiefs of Police Association. MPI provides training and model policies and procedures for police agencies. This policy is an edited version of MPI Policy 1.21, "Use of Mobile Data Terminals (MDT's)."

GENERAL CONSIDERATIONS AND GUIDELINES

The advent of computer access to Criminal Justice Information Sharing (CJIS) and Department records from police vehicles has put a powerful tool into the hands of police employees. Access to CJIS and the gateway to national files are controlled by the Criminal History Systems Board (CHSB), under an agreement with the Federal Bureau of Investigation (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 Lexington Police Officers with guidelines for the proper use of Laptop Computers (sometimes referred to as "Mobile Data Terminals" or "MDTs"). 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.

- A. It is the policy of the Lexington Police 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, research and investigations;
 3. Employees are responsible for ensuring that mobile computers are used in an effective, efficient and lawful manner;
 4. Random and periodic audits of laptop use and log files will be made at the Department's discretion; and
 5. The security and safety of mobile computers is a top priority for employees assigned this equipment.

DEFINITIONS

- B. **MDT: Mobile Data Terminal (LAPTOP):** A cruiser-mounted or otherwise portable computer used by trained and certified department members for purposes of accessing Criminal Justice Information System, Criminal History Systems Board, Law Enforcement Administrative Processing System records, police department information systems or other available information via secure access to various information bureaus.
- C. **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.
- D. **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.
- E. **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.
- F. **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 department policy **82B- Criminal Offender Record Information**.

- G. **LEAPS:** Law Enforcement Administrative Processing System

PROCEDURES

A. Hardware

1. Computers connected to mobile application software will generally be mobile (laptop) computers.
2. Computer connectivity to the mobile system may be accomplished by:
 - a. Laptops with built in modems; or
 - b. Laptop air card.
3. Servers, which run mobile applications, are 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:
 - i. Criminal Justice Information System – CJIS Web;
 - ii. Crimetrack PROIV;
 - iii. Microsoft Outlook;
 - iv. Internet explorer;
 - v. Microsoft word.
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.
 - b. Authorized software may not be manipulated or altered on any agency-owned mobile or desktop. Modifying computer settings, such as changing Windows, or Crimetrack 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.

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 is obtained from the Department authorized Criminal Justice Information System Representative.

D. Use

1. At the beginning of the shift, employees shall check the laptop computer while completing their routine vehicle checks. Damaged equipment must be reported to a supervisor immediately.
2. Employees should log onto the assigned computer and complete their vehicle checklist after roll call. The system should remain active 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 Commanding Officer.
3. All mobile computing transactions must conform to FCC guidelines regarding radio transmissions and shall not contain improper language or subject matter.
4. Officers who obtain actionable CJIS information through the computer such as a "HIT" (warrant, revoked license or registration) **must have the query run through Dispatch to obtain a paper copy of the "HIT" and to confirm accuracy.**
5. Use of the computer should be avoided while the vehicle is in motion, as this may divert the officer's attention from the safe operation of the vehicle. The preferred method when a vehicle is in motion is to run a query through Dispatch.
6. No food, beverage or any other substance that may inflict damage will be placed on or near the computer.
7. 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.
8. 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, this includes disinfectant wipes, as they often cause hazing or damage to the screen. If further cleaning is required, notify the Commanding Officer or Police Mechanic.

9. To ensure that officers' accounts are not accessed, officers must log off of the computer at the end of their tour.
10. All computer inquiries will be done for **legitimate police operations**. All users are prohibited from querying any person or vehicle for personal reasons or simple curiosity. The querying of high profile individuals will trigger an immediate audit by the Commonwealth of Massachusetts and/or the Federal Government.

E. Security

1. Vehicle Mounted computers:
 - a. All cruisers equipped with computers shall be locked whenever unoccupied.
 - b. Laptop computers should be removed from any vehicle, which is anticipated to be out of service for an extended period of time.
 - c. Computers should be rendered non-functional when a vehicle is sent to be repaired by a non-municipal repair facility. They may remain in the vehicle when municipal employees service the vehicle.
 - i. In all cases, computers may be removed from the vehicle.
 - ii. Computers equipped with air cards may have the air cards removed.
 - d. If a computer or air card is discovered to be lost or stolen, this shall be reported immediately to the Commanding Officer, who will make sure the proper steps are taken 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 their Commanding Officer immediately. 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 Criminal History Systems Board.ⁱ
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.ⁱⁱ

F. Training

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

2. Criminal Justice Information System users are required to be trained, tested, and certified, at the minimum, to the “Admin and Query” level of use.ⁱⁱⁱ

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 Department policy **13A-Computers, Security and General Management**.
2. The mobile software logs, mobile communications and data queries may be public records and may have to be released upon receipt of a public records request. For more information see Department policy **82A-Records Management**.

H. Trouble Shooting

1. Computer won't power on:
 - a. Check for battery light and power to the system. The computers are hard wired to the cars.
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 30 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” or “numbers 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 access is connected to the provider.
 - b. If access is not connected try to “connect” by pressing the radio button that states connect. If this is not successful try to reboot the system.
 - c. If the computer is equipped with an air card, (none of the marked units have air cards) 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 Criminal Justice Information System data back:
 - a. Check with other officers to see if they are having difficulty as well.
 - b. Multiple vehicle problems indicate a network or server issue.

ⁱ Appendix D, CJIS Users Agreement.

ⁱⁱ M.G.L. c. 266, §120F.

ⁱⁱⁱ CJIS User Agreement, 3.18.