

DEPARTMENT GENERAL ORDER 04-06

OFFICE of the CHIEF OF POLICE
REPLACES/AMENDS: None

DATE: March 31, 2004

MOBILE DATA TERMINALS

I. PURPOSE.

To establish department guidelines governing the effective and proper use of Mobile Data Computer Systems. Such systems are designed to allow authorized users to access various federal, state, and local Criminal Justice Information Service databases. These networks shall include, but not be limited to: the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), the Missouri Uniform Law Enforcement System (MULES), the Missouri Department of Revenue (DOR) the Regional Justice Information Services (REJIS), and the St. Louis County Police Department Mobilenet Site.

II. DEFINITIONS.

Mobile Data Computer System – The computers, hardware, software and other components that comprise the MDCS.

Mobile Data Terminal – A computer, normally a laptop or handheld, assigned to an officer or officers, individually or to a unit, as part of their assigned field or vehicle equipment.

MDT User – A member of the police department granted the authority to both access and use the department's MDCS.

III. ROUTINE MDT USAGE.

Members of this department shall only use the Mobile Data Computer System if they have successfully completed the required orientation and received proper access authorization.

A. System Activation Required

Each tour of duty, authorized MDT users are required to access the MDCS to ensure the system is functional.

Officers are required to remain connected to the MDCS throughout their tour of duty to the maximum extent possible.

B. Inquiry Protocol

The MDT should be used as the employee's primary access to the previously listed Criminal Justice Information Networks, taking into consideration system availability, time, urgency, and safety.

C. Messaging

All communications via MDT will be professional and shall be conducted in a business-like manner. The transmittal of any sexist, racist, vulgar, derogatory, defamatory, discriminatory, or derogative messages is expressly forbidden. Users are also prohibited from any language that creates an intimidating, hostile, or offensive working environment.

D. Wanted/Warrant Confirmations

MDTs allow individual patrol officers to initiate computer inquiries for wanted persons or objects. When an outstanding warrant or wanted is indicated, the following procedure shall be followed:

- 1). The officer will notify ECDC Dispatch Center that they are out with a wanted subject or vehicle, and provide the location and listed offense.
- 2). The dispatcher shall then confirm that the wanted or warrant is still active with the originating agency.
- 3). An arrest will be made for the wanted/warrant only upon receipt of confirmation.

If there could be a compromise of safety, perceived or real, in any particular situation related to the use of the MDT, the officer is expected to use radio communications.

At the end of the shift, officers should turn off all running programs by selecting "Exit/Close" options, or by using the "X" Icon at the top right corner of the open application. Officers will then turn the computer off to prevent the battery being drained of power.

Should a technical or usage problem arise, officers should consult the Mobile Data Terminal Manual. Copies of the reference manual will be maintained in various locations within the department and will be accessible at all times.

IV. MDT USAGE RESTRICTIONS.

No element of this general order is intended to prohibit or limit a user from making safety conscious decisions. When operating a vehicle, the safe operation of the vehicle is the officer's primary responsibility. Use of the MDCS is always of secondary importance, and the officer will routinely evaluate the need to pull into a parking lot, or out of a traffic lane before activating the system, if such use could divert the driver's attention from the safe operation of the police vehicle.

A. Compliance with City and Department Computer Policies

All users of the Mobile Data Computer System shall be required to adhere to existing City and Department policies governing the proper and sanctioned use of City computer systems.

B. Abuse of Equipment

Department employees shall not abuse MDT equipment. This will include but not be limited to:

1. Do not place objects on the keyboard or MDT lid.
2. Do not shut lid of the laptop until the clasp closes as the securing brackets will break the screen.

B. Message Restrictions

All messages shall be limited in length and duration necessary to accomplish the task or communicate effectively.

Instructions regarding procedural operations of MDT's such as how to log on, how to run inquiries or commands for operating the MDT, must not be broadcast by radio.

C. Release of Information

Officers and other department employees shall not release Criminal Justice System information obtained via MDT, nor shall they release DOR information obtained in the same manner. Requests for information shall be referred to the Records Division.

V. MDT SYSTEM SECURITY AND MAINTENANCE.

It shall be the assigned member's responsibility to ensure the security of the MDT against unauthorized use. Employees shall not give their passwords to any unauthorized person, nor will they leave their password in a written form in or near their computer.

(Authorized persons are defined as MIS employees, REJIS employees assigned as system administrators, and departmental supervisory or command staff).

It shall be the assigned user's responsibility to physically safeguard the MDT using every available precaution (e.g. locking vehicle doors).

Users shall secure their MDT display so that unauthorized persons may not view the data contained on the screen.

Department personnel who temporarily leave an MDT unattended will, except in emergency situations, log out of the system or lock their computer from unauthorized use and viewing.

A. Hardware or Software Modifications

No MDT user or other department employee, unless specifically authorized by the Director of MIS, or his designate, shall make any modifications to the MDT system, the vehicle or field MDT set-up, or to MDCS software, except for user defined options.

No unauthorized software will be loaded on the computers.

B. Monitoring of Equipment Usage

All MDT communications and inquiries shall be for official business only. MDCS communications may be monitored electronically and recorded for future review by MIS or department supervisory staff.

The computer resources and passwords given to MDT users are to assist them in the performance of their duties. Officers do not have privacy, nor should they have any expectation of privacy, in anything they create, store, send, or receive on the system.

C. Equipment Inspections

Computer terminals assigned to department vehicles and/or officers as part of the Mobile Data Computer System, will be subject to periodic line and staff inspections in accordance with established timelines and procedures.

Should a question arise as to an impropriety involving MDT equipment, MIS and supervisory personnel are fully authorized to initiate an immediate inspection of MDT hardware and/or software assigned to a specific vehicle or officer.

D. Malfunction Reporting

MDT users shall notify the Administrative Division supervisor and MIS personnel as soon as practical whenever the Mobile Data Computer System is malfunctioning, has been damaged, lost, or stolen, or whenever unauthorized access is believed to have occurred.

In those cases where the equipment has been damaged, lost, or stolen, the event will be documented by the appropriate incident report or memorandum.

Violation of MDT security policy or associated operating rules which occurs as a result of a deliberate action or personal negligence may result in disciplinary action, up to and including dismissal.

BY ORDER OF:

THOMAS J. BYRNE
Chief of Police

TJB:dld

CALEA Reference: 41.3.7