

NEW CANAAN POLICE DEPARTMENT

SUBJECT: MOBILE DATA TERMINAL'S (MDT'S)



DIVISION ORDER NUMBER: 05-01-03
FILE: SRVS 2.5

I PURPOSE

The purpose of this policy is to provide guidelines for the management and use of the Department's Mobile Data Terminal (MDT) System.

II POLICY

The availability and use of mobile data terminals within the work environment provides many opportunities for enhancement of productivity and effectiveness. This technology also entails the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on the Department, its members, and the public if not managed properly. Therefore, it is the policy of the New Canaan Police Department that all personnel abide by the guidelines set forth herein when using mobile data terminals and the information services that accompany them.

III DEFINITION

Mobile Data Terminal (MDT) - A communications device capable of receiving and transmitting data among terminals and the New Canaan Police Department's Communications Center. A MDT also provides direct user access to national, state and local computer databases and others on the MDT system.

IV PROCEDURES

A. Authority and Responsibility

1. The Computer Systems Administrator shall be responsible for functions including, but not limited to;
 - a. Installation of computers and hardware in designated department vehicles.
 - b. Maintenance and repair of computers and hardware within the MDT System.
 - c. Password assignment and security.
 - d. Software installation and upgrades as required.
2. Before using mobile data terminals, personnel must successfully complete NCIC Criminal Justice Information Service training.

3. Department personnel are authorized to use the MDT System for official Department business as follows:
 - a. Accessing criminal justice information data in the performance of law enforcement duties.
 - b. Accessing other department information files as may be available.

B. Operation

1. The MDT shall be turned on and logged into the system at the earliest opportunity following roll call of each officer's shift. The MDT will remain on at all times that the officer is in his/her patrol cruiser.
2. In the event that the MDT is found to be non-operational or malfunctioning, the officer shall follow only the guidelines set out by the Computer Systems Administrator to troubleshoot the problem.
3. In the event that troubleshooting efforts are ineffective, the officer shall inform Dispatch that the MDT is not fully operational. The officer shall also notify NCPDITHELP via e-mail and copy the message to the Captain of Staff Services. In the message, the officer should be as specific as possible in describing the error so that appropriate personnel can rectify it.
4. Officers should consider safety concerns while on traffic stops and when confronting suspects before focusing attention on the MDT. Back-up officers and criminal justice information requests through the communications center should be used when appropriate.
5. Personnel are prohibited from using MDT's while the vehicle is in motion. Department members who are passengers in a vehicle are not included in this prohibition.
6. Officers should recognize the inherent risk to the life of the MDT's when they are left on for extended periods of time. To preserve the life of the hardware, officers should shut down the MDT's at the end of each shift and when they are going to be away from the vehicle for an extended period of time (i.e. 20 minutes or more).
7. Officers shall follow the procedures defined by the Computer Systems Administrator to shut down the MDT.

C. NCIC

1. All access of NCIC databases shall be performed in compliance with established FBI regulations.
2. Officers should be aware of Federal and State guidelines regarding NCIC operation and security. Officers should not leave NCIC in active mode when they are not able to monitor the screen.
3. Wanted persons, stolen vehicles, and any other type of "Hit" obtained through NCIC shall be confirmed through the communications center.
4. Officers should use their MDT to conduct routine vehicle and/or person checks in order to relieve Communications personnel workload and to reduce radio traffic.

D. Law Enforcement Administration System (LEAS)

1. The MDT provides officers with all functions of LEAS software that are available on the department's in-house computers.
2. Officers should, whenever possible, complete all reports in the vehicle, per the shift commander. Motor vehicle accident reports and exceptionally detailed reports may be exempted from this rule.
3. Officers shall notify Dispatch of their location when they set to complete reports in the vehicle and shall also notify Dispatch when they clear from their reports.

E. Computer Aided Dispatch (CAD)

1. The MDT will be used in conjunction with radio communications and is not intended to be a replacement for voice dispatching.
2. The MDT may be used to reduce radio communications, enhance officer safety and provide a means of transmitting information and messages.

F. Security

1. Criminal justice information, which can be accessed through the MDT System, is not public information and shall be accessed for law enforcement purposes only.
2. Information displayed on the MDT screen is confidential in nature and officers should take appropriate measures to ensure the information is not readily in view of the public.
3. Officers assigned vehicles with MDT's shall be responsible for ensuring that unauthorized use of the unit does not occur.
4. Vehicles equipped with MDT's shall be locked when not either in operation or occupied by an authorized user.

G. Safety

1. The computer, keyboard, and screen installation in every Ford Crown Victoria in the department fleet is compliant with airbag safety standards.
2. Officers may utilize adjustable brackets to reposition the keyboards in every Crown Victoria to their comfort while stationary for reports. When in operational mode, the keyboards must be positioned to adhere to airbag safety standards.

V DISTRIBUTION

This division order will be reproduced in electronic and traditional media. All sworn personnel shall have access to Department general orders through a read-only file on their individual domain of the Department's computer network. Printed copies will also be placed in locations throughout headquarters so that they are easily accessible to all personnel.

VI **EFFECTIVE DATE**

This division order approved by the Police Commission on May 18, 2005 and is effective May 19, 2005.

Reviewed December 2005

Per Order

Edward J. Nadriczny
Chief of Police