FREDERICK POLICE DEPARTMENT
GENERAL ORDER

Section 9: Police Equipment and Vehicles **Order Number:** 978
Topic: MOBILE DATA TERMINAL SYSTEM **Issued by:** Chief of Police
Approved: 01/09/19
Review: Annually in November by the Technology and Services Division Commander
Supersedes: GO 978 dated 11/8/16

.01 PURPOSE:

To establish departmental policy, procedures, and minimum guidelines concerning the operation and use of the mobile data terminal (MDT).

.02 CROSS-REF:

G.O. 975, "Automated Information System (AIS)"
FBI CJIS Security Policy

.03 DISCUSSION:

A mobile data terminal (MDT) is a communications device capable of receiving and transmitting data among units and the Frederick Police Department Communications Section. A MDT also provides direct user access to national, state, and local computer databases and others on the MDT system.

.04 POLICY:

The use of Department MDTs will be in accordance with FBI CJIS Security policy, and limited to those operations that support the Department mission.

.05 DEFINITIONS:

Criminal Justice Conveyance: Any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods with CJIS security policies.

Physically Secure Location: A physically secure location is a facility, a criminal justice conveyance, or an area, a room or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

.10 GENERAL:

1. In any police vehicle in which a MDT is installed, the MDT will be turned on and logged into the system at the beginning of each officer's shift. The MDT will remain on at all times that the officer is on-duty. The driver of any vehicle will not operate a computer while the vehicle is in motion. Solo officers assigned MDTs will stop their vehicle and park in a safe manner before attempting to access information.

2. MDT users are forbidden from modifying default settings, e.g., font size, pixel count, creation of a windows password, etc. and loading of any unauthorized software.

3. Officers are required to use the MDT to make all CJIS/NCIC/METERS inquires unless circumstances exist that make using the MDT impractical or a danger to officer safety. The MDT will be used in conjunction with radio communications and is not intended to be a replacement for voice dispatching. Warrant information received from the MDT will *NOT* be considered probable cause for arrest until properly verified and confirmed by a Dispatcher per Communications procedures.

4. Responses from inquires to CJIS/NCIC/METERS are protected information. Officers are

not permitted to use these systems for their own use, and information received through these computer systems may only be used for official criminal justice purposes. Officers will not initiate any inquiry outside those purposes necessary to complete a departmental objective. Officers will ensure that unauthorized persons, to include passengers or offenders located in the vehicle, do not view responses from these systems.

5. In any police vehicle in which a MDT is installed, special care will be taken to prevent spillage of foreign objects onto the MDT equipment. Beverages and other containers will be secured with lids.

.15 ELECTRONIC MESSAGING PROCEDURES:

1. Electronic messages sent on the MDT will be for Department business purposes only. Short personal messages are allowed as long as they are not offensive, degrading or embarrassing in any way to the Department or any individual. Under no circumstances will an employee using the MDT system broadcast jokes, sexual comments or innuendos of a provocative or suggestive nature, or language that creates an intimidating, hostile or offensive working environment of any kind. Supervisory staff, to assure proper procedures are being followed, will periodically review the message logs.

2. Any electronic message that is sent through the MDT system may be retrieved by authorized personnel later, even though it may have been deleted from the assigned employee's computer. Electronic messages are not a protected form of communication and could be subject to a discovery motion in a criminal/civil case or an internal investigation.

3. Every electronic message should be considered in the public domain. Assigned employees should have no expectation of privacy regarding electronic messages. All electronic messages will be professional and courteous.

4. Personnel status notifications, e.g., in service and/or out of service, will not be communicated by electronic messaging on MDTs because acknowledgement of such transactions may not occur in a timely fashion.

.20 SECURITY/STORAGE:

1. It will be the assigned employee's responsibility to safeguard the computer by ensuring it is locked in the docking station, as well as locking the vehicle upon exiting the vehicle. All personnel are required to log off from all network computer systems at the completion of their workday.

2. If a MDT needs to be removed from a vehicle the user will do so within a physically secure location or will log out of MPS and manually initiate a screen/session lock while the computer is in transport outside of a physically secure location. Users are not authorized to access CJIS while outside of a physically secure location or criminal justice conveyance.

3. Any use of a Department computer by anyone other than an authorized user is prohibited. It will be the assigned employee's responsibility to ensure the security of the computer against unauthorized use. Employees will not give their passwords to any other person or persons to use, nor will they leave the password in any discernible written form in or near their computer. Individuals will be held strictly accountable for any transaction appearing under their log on signature and password. Assigned personnel, however, may be required to disclose this information to someone in their chain of command or support personnel for departmental business purposes.

4. Personnel leaving employment with the Department will have their MDT access accounts deleted. It is the employee's direct supervisor's responsibility to notify the Commander or

Manager of the Technology and Services Division for account deletion.

5. The Commander or Manager of the Technology and Services Division will be responsible for maintaining an inventory of all MDTs, and will conduct an annual inspection of all vehicle-mounted MDTs during the month of July.

6. The assigned officers will conduct a daily inspection of the MDT. Any non-functioning or malfunction MDT (hardware/software) will be noted on the vehicle inspection form and forwarded to the Vehicle Fleet Coordinator. The coordinator will in turn forward all information relative to MDTs to the Commander or Manager of the Technology and Services Division.

.25 MAINTENANCE:

1. The Technology and Services Division is responsible for all maintenance, support, and repair of the MDTs. Under no circumstances will officers attempt to repair or correct problems with the MDTs. Requests for service will be recorded on the vehicle inspection form which is forwarded via chain of command and will include the following information:

   A. a detailed description of the problem;

   B. the date and time of occurrence;

   C. whether or not the problem can be duplicated on the same computer or another computer; and,

   D. what steps, if any, were taken to resolve the problem.

2. After regular business hours, supervisory personnel have the authority to contact the Commander or Manager of the Technology and Services Division to resolve *major* system failures.

3. The Commander, TSD, or his/her designee will conduct periodic system-wide audits as directed by the Chief of Police, or upon formal request by a supervisor for a specific transaction. Additionally, in order to conserve computer storage space, the Commander or Manager of the Technology and Services Division will purge the system of stored transactions as needed.

.30 EMERGENCY ACTIVATION:

1. The silent signaling of an emergency by MDT is not encouraged as a first line action and should only be used as a last resort. Whenever possible the silent signaling of an emergency should be via voice radio system since it has the most effective attention-evoking alert to the on-duty dispatcher.

2. Each MDT is equipped with an “emergency button” which, if activated, will alert everyone signed onto the system. If activated, all units will proceed as if the activating officer is in a true emergency and will proceed appropriately.

.40 TRAINING:

1. The Commander or Manager of the Technology and Services Division is responsible for granting access to the MDT system.

2. Access to METERS/NCIC can only be granted after completion of the mandated training course. It will be the responsibility of the employee to maintain METERS/NCIC certification if required by the employee’s supervisor or specific job assignment.

3. Personnel assigned to the Training Unit will be responsible for coordinating appropriate

computer training specific to the software available to the assigned employee.