2.464 MOBILE DATA TERMINAL SYSTEM

2.464.10 Policy

It shall be the policy of the University of Maryland, Department of Public Safety to use the Mobile Data Terminal (MDT) System to support the Department's activities. It is the responsibility of each user to ensure that this technology is used for proper business purposes and in a manner that does not compromise confidential, protected, restricted or otherwise sensitive information.

2.464.20 Mobile Data Terminal Program Coordinator

The Chief of Police will designate an MDT Program Coordinator. The MDT Program Coordinator will ensure that the required employees are trained on the proper use of the MDT and will work closely with the Information Systems Unit in equipment maintenance. The MDT Program Coordinator will be responsible for reviewing the MDT system use if they are made aware of any MDT System usage violations.

2.464.30 General MDT System Usage

A. All MDT's, data and software, maintained or used by the University of Maryland, Department of Public Safety are for official use only. No employee will use or cause to be used any MDT for personal gain or benefit of any kind.
B. No employee will attempt to install, delete or modify any software or hardware associated with the MDT at anytime consistent with **1.1006 Information Systems Security and Acceptable Use**. This includes, but is not limited to, modifying any default settings, e.g., font size, pixel count, etc.
C. If any equipment needs to be serviced, a message will be sent using the IT request form on a UMPDS computer.
D. Users will be responsible for inspecting the MDT at the beginning of each shift. If any damage is noted, an e-mail must be sent using the IT request form on a UMDPS computer along with an email to the user's supervisor. If the damage has not been previously reported, the previous user will be held accountable.
E. It will be the responsibility of each officer or civilian employee with access to the MDT System to keep their system logon and password current.
F. Any user who violates any of the policies or rules set forth in this directive will be subject to removal or suspension from the program and may face further disciplinary sanctions.
G. The use of the MDT while operating agency vehicles on the roadway is prohibited.
    1. The MDT screen should be closed when the vehicle is in operation to prevent distraction to the operator.
    2. Requests for information normally accessed through the MDT during times at which the operator is driving should be made to Communications.

2.464.40 Mobile Data Terminal Procedures

A. All electronic messaging/correspondence is the property of the University of Maryland Department of Public Safety.
B. Mobile Data Terminal usage is restricted to those agency employees who have been trained in the proper usage of the equipment and who have been granted access to the system.
C. User passwords to access the MDT System, MILES/NCIC System, and the Prince George's County Sheriff's System shall not be shared or made known to any other individual. Assigned users may be required to disclose this information to someone in their chain of command or computer support personnel for business purposes. Users who believe that their password has been compromised shall immediately notify the MDT Program Coordinator and copy their immediate supervisor. Attempts by any member to utilize an MDT or gain access to any of the systems with another user's password are strictly prohibited.
D. The safe operation of a police vehicle shall always be the driver's primary responsibility and they must give full time and attention to the operation of the vehicle. The use of the MDT shall always be secondary to the safe operation of the vehicle. Drivers shall carefully consider the need to safely stop the vehicle before using the MDT if such use is going to divert the user's attention from the safe operation of the vehicle. In motion MDT usage is only authorized when it will not impair the driver's ability to operate the vehicle, and shall generally be limited to:
    1. Running a time-sensitive inquiry (i.e. 10-28, 10-29)
    2. Limited keystrokes, acknowledging a message, when a delay would be unreasonable.
E. Collisions involving the use of the MDT in violation of this policy will be handled consistent with **2.900 Complaints & Discipline**.
F. A user receiving a 10-99 "hit" must verify the hit by viewing the NCIC Summary Screen to ensure that the hit is identical for the person, property or vehicle that the user entered, prior to initiating a stop, contact or other enforcement activity, unless other probable cause exists for a stop. Users must then confirm the hit (i.e. confirm the existence of an open warrant or stolen vehicle,etc.) through communications.
    1. A computer hit is not sufficient probable cause to make an arrest.
    2. Barring exigent circumstances, an arrest shall not be made until the hit is confirmed.

2.464.50 Electronic Messaging Procedures

A. All electronic messages should be considered in the public domain. Employees should have no expectation of privacy regarding electronic messages. All transactions on the MDT are electronically logged. All electronic messages should be professional. They should not be 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. The MDT Program Coordinator, or other Supervisory employees, will periodically review the message logs.
B. 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 specific MDT. 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.

2.464.60 Security/Storage of Mobile Data Terminals

A. It will be the responsibility of an assigned employee to safeguard the computer by locking the vehicle upon exiting the vehicle. All personnel are required to log off from all network computer systems and programs at the completion of their work day.
B. The MDT Program Coordinator will be responsible for maintaining an inventory of all MDT's and will conduct a annual inspection of all vehicle mounted mobile computers.
C. Employees will keep the MDT screen and keyboard clean using the supplies provided. Employees will not use any items that may damage the MDT, (i.e. scratch the monitor).
D. Food and liquids must be kept away from the MDT's at all times. In the event of a spill, the employee will:
    1. Log off all active sessions and shut down the MDT as quickly as possible.
    2. Clean the affected area as soon as possible by wiping the spill.
    3. Notify the MDT Program Coordinator and the employee's immediate supervisor immediately for corrective action.

2.464.70 Mobile Data Terminal Operational Procedures

A. Definitions:
   1. Confirmation: Process of communications personnel contacting originating agencies for wanted and stolen hits received through NCIC or MILES.
   2. Verification: Process of officers requesting communications personnel run registration, stolen or wanted checks through the communications terminal to affirm information officers read on MDTs.

B. Officers will maintain MDT certification and keep passwords and access levels (NCIC, MILES, PGSO, etc) current and up to date.

C. Upon going in-service for patrol or other traffic enforcement duties, Officers will notify communications of the status of their MDT.

D. Officers will utilize MDTs for routine registration, stolen, wanted and drivers license checks whenever possible to relieve communications staff of this responsibility.

E. Information read from MDT vehicle registration checks will constitute probable cause to make traffic stops and issue traffic citations for violation of the traffic articles. Warrant hits, or information relating to the registered owner of a vehicle (suspended, revoked, unlicensed) will NOT constitute probable cause for a traffic stop.

F. Information read from MDT driver's license checks will constitute probable cause to issue traffic citations for violations of the traffic articles.

G. Communications staff will make attempts to run registrations of vehicles on which officers make traffic stops, conduct assist motorist, or are stopped for other investigative reasons.

H. Officers making stops on vehicles will notify communications if the officer is aware of any confidential information on the registration of that vehicle. Communications will notify officers of confidential information if officers do not notify Communications that they are already aware of the information.

I. Officers will have Communications confirm stolen and NCIC/MILES wanted hits before making arrests..

J. Officers will have Communications personnel verify PG Sheriffs wanted hits on the Communications terminal before making arrests.