

Mobile Data Terminal Use

423.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper access, use, and application of the Mobile Data Terminal (MDT) system in order to ensure proper access to confidential records from local, state, and national law enforcement databases, and to ensure effective electronic communications between department members and Communications. See the CJIS Access, Maintenance, and Security Policy 809 for additional guidance.

423.2 POLICY

University of Maryland, Baltimore Police Department members using the MDT shall comply with all appropriate federal and state rules and regulations and shall use the MDT in a professional manner, in accordance with this policy.

423.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to messages accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use Policy 321 for additional guidance).

423.4 RESTRICTED ACCESS AND USE

MDT use is subject to the Information Technology Use, Protected Information, and CJIS Access, Maintenance, and Security policies (321, 805, and 809).

Members shall not access the MDT system if they have not received prior authorization and the required training. Members shall immediately report unauthorized access or use of the MDT by another member to their supervisor or Shift Commander.

Use of the MDT system to access law enforcement databases or transmit messages is restricted to official activities, business-related tasks, or communications that are directly related to the business, administration, or practices of the department. In the event that a member has questions about sending a particular message or accessing a particular database, the member should seek prior approval from their supervisor.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing, or any other inappropriate messages on the MDT system is prohibited and may result in discipline.

It is a violation of this policy to transmit a message or access a law enforcement database under another member's name or to use the password of another member to log in to the MDT system unless directed to do so by a supervisor. Members are required to log off the MDT or secure the MDT when it is unattended. This added security measure will minimize the potential for unauthorized access or misuse.

Mobile Data Terminal Use

423.4.1 USE WHILE DRIVING

Use of the MDT by the vehicle operator should be limited to times when the vehicle is stopped. Information that is required for immediate enforcement, investigative, tactical or safety needs should be transmitted over the radio.

In no case shall an operator attempt to send or review lengthy messages while the vehicle is in motion.

423.5 DOCUMENTATION OF ACTIVITY

Except as otherwise directed by the Shift Supervisor, all calls for service assigned by a police communications operator should be communicated by voice over the police radio and electronically via the MDT unless security or confidentiality prevents such broadcasting.

MDT and voice transmissions are used to document the member's daily activity. To ensure accuracy:

- (a) All contacts or activity shall be documented at the time of the contact.
- (b) Whenever the activity or contact is initiated by voice, it shall be documented by a police communications operator.
- (c) Whenever the activity or contact is not initiated by voice, the member shall document it via the MDT.

423.5.1 STATUS CHANGES

All changes in status (e.g., arrival at scene, meal periods, in service) will be transmitted over the police radio or through the MDT system.

Members responding to in-progress calls shall advise changes in status over the radio to assist other members responding to the same incident. Other changes in status can be made on the MDT when the vehicle is not in motion.

423.5.2 EMERGENCY ACTIVATION

If there is an emergency activation and the member does not respond to a request for confirmation of the need for emergency assistance or confirms the need, available resources will be sent to assist in locating the member. If the location is known, the nearest available officer should respond in accordance with the Officer Response to Calls Policy 309.

Members should ensure the Shift Supervisor and Shift Commander are notified of the incident without delay.

Officers not responding to the emergency shall refrain from transmitting on the police radio until a no-further-assistance broadcast is made or if they are handling a different emergency.

423.6 EQUIPMENT CONSIDERATIONS

423.6.1 MAL-FUNCTIONING MDT

Whenever possible, members will not use vehicles with malfunctioning MDTs. Whenever members must drive a vehicle in which the MDT is not working, they shall notify Communications.

Mobile Data Terminal Use

It shall be responsibility of the police communications operator to document all information that will then be transmitted verbally over the police radio.

423.6.2 BOMB CALLS

When investigating reports of possible bombs, members should turn off their MDTs when in close proximity of a suspected explosive device. Radio frequency emitted by the MDT could cause some devices to detonate.