



Approved:

*Chief Marcia Harnden*

Subject:

# 632. Mobile Data Terminals

Effective:

December 13, 2017

CALEA Standards: 41.3.7

Page:

1

## 632.1: 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 appropriate access to confidential records from local, state and national law enforcement databases, and to ensure effective electronic communications between department members and the Communications Center.

## 632.2: POLICY

**Albany 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.**

## 632.3: PRIVACY EXPECTATION

- a. Communication via MDTs between employees is limited to legitimate law enforcement use and could be determined to be public information.
- b. 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 630](#) for additional guidance).

### 632.3.1: SUPERVISORY REVIEW

Supervisors of employees who regularly use MDTs should periodically conduct an audit of their employees' MDT messages to ensure compliance with this policy.

## 632.4: RESTRICTED ACCESS AND USE

- a. MDT use is subject to the Information Technology Use: Policy 0630 and [Records Maintenance and Release: Policy 601](#) policies.
- b. Members shall not access the MDT system if they have not received prior authorization and the required training.
- c. Members shall immediately report unauthorized access or use of the MDT by another member to a supervisor.

- d. Use of the MDT system to access law enforcement databases or transmit messages is restricted to official activities, business-related tasks and communications that are directly related to the business, administration or practices of the Department.
  - 1) 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 his/her supervisor.
- e. Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing or any other inappropriate messages on the MDT system is prohibited and may result in discipline.
- f. Members shall not transmit a message or access a law enforcement database under another member's name or use the password of another member to log in to the MDT system unless directed to do so by a supervisor.
- g. To minimize the potential for unauthorized access or misuse, members shall log off the MDT or secure the MDT when it is unattended.
- h. Any agency using a terminal to access the Law Enforcement Data System (LEDS), whether directly or through another agency, is responsible for adhering to all applicable LEDS rules and policies and must ensure that unauthorized persons are not given access or allowed to view LEDS information.

#### **632.4.1: USE WHILE DRIVING**

- a. Use of the MDT by the vehicle operator should be limited to times when the vehicle is stopped.
- b. Information that is required for immediate enforcement, investigative, tactical or safety needs should be transmitted over the radio.
- c. In no case shall a vehicle operator attempt to send or review lengthy messages while the vehicle is in motion.

#### **632.5: DOCUMENTATION OF ACTIVITY**

- a. Except as otherwise directed by the Watch Supervisor, Shift Supervisor, or other department-established protocol, "Priority 1" and "Priority 2" calls for service assigned by a Communications Specialist should be communicated by voice over the police radio and electronically via the MDT unless security or confidentiality prevents such broadcasting.
- b. MDT and voice transmissions are used to document the member's daily activity. To ensure accuracy:
  - 1) All contacts or activity shall be documented at the time of the contact;
  - 2) Whenever the activity or contact is initiated by voice, it shall be documented by a Communications Specialist;

- 3) Whenever the activity or contact is not initiated by voice, the member shall document it via the MDT.

#### 632.5.1: STATUS CHANGES

- a. All changes in status (e.g., arrival at scene, meal periods, in service) should be transmitted over the police radio or through the MDT system.
- b. Members responding to in-progress calls should advise changes in status over the radio to assist other members responding to the same incident.
- c. Other changes in status can be made on the MDT when the vehicle is not in motion.

#### 632.5.2: EMERGENCY ACTIVATION

- a. 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.
  - 1) If the location is known, the nearest available officer should respond in accordance with the [Patrol Function: Policy 220](#).
- b. Members should ensure the Shift Supervisor or Watch Supervisor are notified of the incident without delay.
- c. Officers not responding to the emergency shall refrain from transmitting on the police radio until a no-further-assistance (Code 4) broadcast is made or if they are also handling an emergency.

### 632.6: EQUIPMENT CONSIDERATIONS

#### 632.6.1: MALFUNCTIONING MDT

- a. When practical, field personnel should not use vehicles without MDTs.
- b. Whenever members must drive a vehicle in which the MDT is not working, they shall notify the Communications Center.
- c. It shall be the responsibility of the Communications Specialist to document all information that will then be transmitted verbally over the police radio.

#### 632.6.2: RESPONSE TO BOMB CALLS

Because radio frequency emitted by MDT's could cause some explosive devices to detonate, members should not communicate via MDT when in the evacuation area of a suspected explosive device (see [Response to Bomb Calls: Policy 430](#)).

