# Mobile Data Terminal Use

## 603.1 VERSION

| Review Date | Effective Date | Approving Authority |
| --- | --- | --- |
| 01/24/2020 | 07/09/18 | Eric D. English, Chief of Police |

## 603.2 POLICY AND PURPOSE

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 employees and Emergency Communications Center. Harrisonburg Police Department employees 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.

## 603.3 ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this policy. Responsibility rests with the supervisor to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated. This directive is for internal use only, and does not enlarge an employee's civil liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this department, and then only in a non-judicial administrative setting.

## 603.4 PRIVACY EXPECTATION

Employees forfeit any expectation of privacy with regard to messages accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use/Electronic Mail policy for additional guidance).

## 603.5 RESTRICTED ACCESS AND USE

MDT use is subject to the Information Technology Use/Electronic Mail and Protected Information policies.

Employees shall not access the MDT system if they have not received prior authorization and the required training. Employees shall immediately report unauthorized access or use of the MDT by another employee to their supervisors or Patrol Commanders.

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 his/her 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.

### 603.5.1  USE WHILE DRIVING
Use of the MDT by the vehicle operator should generally be limited to times when the vehicle is stopped. When the vehicle is in motion, the operator should only attempt to read messages that are likely to contain information that is required for immediate enforcement, investigative or safety needs.

Short transmissions, such as a license plate check, are permitted if it reasonably appears that it can be done safely. In no case shall an operator attempt to send or review lengthy messages while the vehicle is in motion.

### 603.6  DOCUMENTATION OF ACTIVITY
Except as otherwise directed by the Patrol Commander or other department-established protocol, all calls for service assigned by a communicator 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 should be documented by a communicator.

>  (c)   Whenever the activity or contact is not initiated by voice, the member shall document it via the MDT.

### 603.6.1  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.

Officers responding to in-progress calls should advise changes in status over the radio to assist other officers responding to the same incident. Other changes in status can be made on the MDT.

### 603.6.2  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 officer. If the location is known, the nearest available officer should respond.

Officers should ensure a field supervisor and the Patrol 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.

## 603.7 EQUIPMENT CONSIDERATIONS

### 603.7.1 MALFUNCTIONING 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 Emergency Communications Center. It shall be the responsibility of the communicator to document all information that will then be transmitted verbally over the police radio.

### 603.7.2 BOMB CALLS
When investigating reports of possible bombs, members should not communicate on their MDTs when in the evacuation area of a suspected explosive device. Radio frequency emitted by the MDT could cause some devices to detonate.