TIVERTON POLICE DEPARTMENT
GENERAL ORDERS

Subject: Mobile Data Terminals (MDT)	**General Order Number:** 320.80	
Section: 300- Law Enforcement Operations	**Subsection:** 20- Patrol	
Amends/Supersedes: 320.80 (01/13/2015)		
Effective Date: 01/13/2015	**Revised Date:** 01/31/2023	**Review Date:** As Needed
Per Order Of: Patrick W. Jones, Chief of Police		
RIPAC: 15.9		
Distribution: Sworn Department Members, Communications Center Operators		

NOTE: This written directive is for the internal governance of the Tiverton Police Department, and is not intended and should not be interpreted to establish a higher standard of care in any civil or criminal action than would otherwise be applicable under existing law.

I. PURPOSE

The purpose of this policy is to establish procedural guidelines for the operation of Mobile Data Terminals (MDT). The Tiverton Police Department system utilizes software that allows members in the field direct access to RILETS, NCIC, internal Records Management System (RMS), and Computer-Aided Dispatch (CAD) information through the use of software running on portable MDTs. This information will be made available to the members without the need for voice interaction with a dispatcher.

II. POLICY

The Tiverton Police Department authorizes the use of MDTs in a lawful, safe, effective and efficient manner only to enhance a police officer's informational effectiveness.

III. DEFINITIONS

MDT: Mobile data terminal, laptop, or tablet used in the field.
Peripheral: A device that is connected to a host computer, but not an integral part of it. It expands the host's capabilities but does not form part of the core computer architecture (e.g. mouse, keyboard, printer, monitor, hard drives, flash drives).
Wireless: Data communications sent and received from the field without the use of hard wires.
IMC (Tritech): Public safety software used both in the field (IMC Mobile) and in-house for records management and report writing (IMC Records) and dispatch (IMC LAN/Dispatch) functions.
RILETS: Rhode Island Law Enforcement Telecommunications System; As defined by Rhode Island General Law (RIGL) 42-28-16, Statewide Police Telecommunications System- "The division of the State Police is authorized and empowered to provide for the installation, operation, and maintenance of a computerized telecommunications system

for the purpose of promptly collecting, exchanging, disseminating, and distributing information relating to police and divisional problems for the state, cities, and towns." "The system is to be installed, operated, and maintained following rules and regulations adopted from time to time by the superintendent of State Police and units thereof located in such state departments and agencies in such cities and towns as have organized police headquarters and are approved by the superintendent, and may connect directly or indirectly with similar systems in other states. The superintendent of State Police is authorized to provide for the location of the receiving system computer site and to employ the necessary personnel for its operations."

IV. PROCEDURES

A. Use, Care, and maintenance of Equipment

Employees will not alter or disassemble any equipment, device, or connection to an MDT, modem, or antenna without the consent of the department's Information Technology (IT) Services Contractors and the Uniform Division Commander (Captain) or designee.

1. Employees assigned an MDT will be responsible for the physical security and general upkeep of that MDT including a daily inspection of the computer and all components. Personnel will immediately notify the Captain of any needed repair, maintenance, or technical operation issues through the appropriate chain of command and document with an interdepartmental communication or internal email.
2. All employees will use every reasonable precaution available to keep the MDT secure (i.e., locking the vehicle when unattended). No employee will allow any unauthorized entry into the vehicle for purposes of interfering with the setup.
3. No food or drink will be placed on or near the MDT where there might be spillage or leakage.
4. No unauthorized software will be installed (either permanently or temporarily) on the MDT. No unauthorized media (CDROM, flash drives, etc.) will be permitted on the MDT at any time. No unauthorized external devices or peripherals will be attached to the MDT at any time. Also refer to General Order #300.70 Computer Systems.
5. No modifications to the original operating system image/format or software applications will be permitted unless authorized by IT Services, and the Captain, or a designee.
6. The MDT shall be physically turned off (programs exited, unit signed off, and powered down) if the vehicle must be jumped started to protect the MDT.
7. All MDTs shall be turned off when not in use.
8. When a vehicle is to be serviced off-site, the department mechanic will ensure that an MDT is not mounted in the vehicle before the vehicle is serviced.

B. General Operation of Equipment

1. When a vehicle is operated as a single officer unit, the safe operation of the vehicle takes precedence over the operation of the MDT. Operation of the MDT does not serve as a mitigating justification in the event of a fleet accident. While undertaking MDT operations, personnel will maintain a

conscious awareness of their surroundings, remain alert to potential hazards and practice safe tactics.

2. All personnel using MDTs are responsible for signing on at the beginning of their tour of duty and signing off at the end of their tour of duty.
3. Communications between mobile units and the Communications Center will adhere to the following criteria:
    a. The initiation of any call for service (with the exception of building checks, beach checks, house checks, and traffic posts) and all motor vehicle stops, if entered in the MDT, must also be communicated orally by radio. This also applies to any situation where officer safety could be a consideration.

C. Care and Use
1. Care
    a. Police vehicles should remain secured at all times when not in use.
    b. Nothing should be placed on top of the MDT, especially any food or drinks.
    c. No unauthorized internet access use, unauthorized electronic data/software, or materials should be loaded into the MDT.
    d. Recommendations dealing with changes or improvements should be reported to the Captain.
    e. The MDT will not be used while the car is in motion unless the vehicle is in operation with two officers. This refers to data entry into the computer; NOT the viewing of the screen while the car is in motion for silent dispatching or viewing the status of other cars. In either case, members are to utilize the radio to notify the dispatcher of the call reason and location before stopping vehicles. While utilizing the MDT, officers shall be mindful of their safety at all times. Officers shall position themselves to observe the stopped motorist or occupants at all times while entering data.
2. Temperature Considerations:
    a. Officers should be mindful of extreme heat or cold and take reasonable action to mitigate the temperature concerning the MDT.

D. Messaging Guidelines
1. All rules and laws that govern radio transmissions are applicable during MDT operations. Departmental directives, policies, and procedures that contain applicable RILETS/NCIC guidelines apply to the operation of the MDT. Information obtained by the operation of the MDT is maintained as confidential information following applicable laws.
2. Queries made through the MDT will be limited to those according to a lawful police function and are to be used for criminal justice purposes only.
    a. All efforts must be made to prevent information sent and received through the MDT from being viewed by any unauthorized individuals. When unauthorized individuals are within viewing distance of the computer screen, the screen must either be off or turned away from the unauthorized individual.

3. Records of all MDT transmissions/activities are recorded and stored by the main NCIC/RILETS system located at Rhode Island State Police Headquarters, and are subject to monitoring and/or retrieval.
    a. All MDT transmissions should be considered as existing in the public domain and should be professional and acceptable as radio traffic if it were on normal radio frequency channels.
    b. Employees will not create messages on any MDT or departmental computer that could be considered obscene, derogatory, racially insensitive, demeaning, or sexual.
    c. Employees have no expectation of privacy of information contained in an MDT in the Police Department domain or any computer on department facilities or vehicles. Any computer system security feature such as passwords or message delete functions does not affect the right of supervisors, IT Services, or the Chief of Police or designee to access information at any time. When requested by the Chief of Police or designee, an employee is required to disclose any passwords or codes necessary to access their MDTS and/or any software applications contained therein.