

THE RALEIGH POLICE DEPARTMENT

1109-17

MOBILE COMPUTER TERMINALS (MCT)

PURPOSE

To provide regulations and procedures governing the use and security of Mobile Computer Terminals.

VALUES REFLECTED

This directive reflects our values of *Service and Integrity*. By observing these guidelines we demonstrate that we adhere to the highest standards for using the best technology available to us. We recognize that with the privileges and work improvements brought to us through technology come the responsibility to use these resources wisely and to everyone's benefit.

UNITS AFFECTED

All Divisions/All Personnel
Emergency Communications Center

REFERENCES/FORMS

DOI 1101-06 "Police Computer Equipment and Software"
DOI 1101-08 "Internet Access, Usage, and Email Standards"
DOI 1106-01 "Confidentiality and Release of Information"
DOI 1106-03 "DCI/NCIC Security and Access"
DOI 1109-01 "Patrol Operations"
DOI 1109-02 "Radio Communications, Response to Calls"

May be Released to the Public

Effective Date: 10-06-14
Prepared By: C.L. Deck-Brown
Chief of Police

Supersedes: 03-15-06
Approved By: Ruffin Hall
City Manager

GENERAL POLICIES

Communication over the Mobile Computer Terminal (MCT) is not intended to replace radio communication, rather to reduce it and make it more efficient. As such, all traffic sent over the MCT must be business related and conform to FCC rules and regulations.

Only personnel who have been trained in the operation of the MCT and have completed a "Raleigh Police Department Personal Computer User Agreement" may attempt to operate the terminal. Additionally, only those personnel who have been certified by the Division of Criminal Information (DCI) may log onto DCI.

Information received from inquiries into DCI, CAD, or any other databases is confidential and may be released to criminal justice personnel only.

Any violation of this policy will result in disciplinary action, up to and including dismissal.

MANAGEMENT OF MOBILE COMPUTER TERMINALS

All MCTs in the Department will be the administrative responsibility of the Police Information Services Manager. The user has the responsibility of promptly reporting malfunctions of the terminal hardware or software to the Police Information Services Manager in person or by memo, telephone, or E-mail.

Staff/Line Inspections

The Information Services staff will conduct periodic inspections of all MCTs. This inspection will cover the physical condition and operational soundness of the terminal.

Additionally, supervisors will inspect each MCT during vehicle inspections for obvious signs of damage.

Training

The Information Services staff will ensure that all affected personnel are trained in the use of the MCT before giving security clearance or access to operate the terminal to any person.

Maintenance

Maintenance to be performed on any terminal will receive prior authorization from Information Services staff. This includes any repair or movement of the terminal itself (hardware) or the installation, deletion, or modification of any interior/exterior components or software.

TERMINALS

Security and Care of Equipment

In order to protect the confidential nature of the accessible information available through the MCT, as well as safeguard the security of our patrol communications systems, officers must always exercise care with the terminal.

- Upon beginning a tour of duty, all officers must inspect the MCT in their vehicle for evidence of obvious tampering.
- Officers must properly log onto both CAD and DCI upon beginning a tour of duty.
- Whenever officers can predict that they will be out of sight of their vehicles, they must secure their vehicles to prevent unauthorized access to the terminal. In addition, the officer must enter a status update of "Not on MCT" with an appropriate location to notify the responsible telecommunicator. When returning to the vehicle, the officer must enter a status of "Return to MCT".
- If an officer is to be away from the vehicle and will not return to the vehicle, they must log off of DCI and CAD. The power switch for the MCT should be turned off also.
- Food and liquids must be kept away from the MCT at all times.
- The power switch to the MCT must be turned off before any attempt is made to "jump start" a vehicle.

General Terminal Operation

Due to the obvious risks associated with attempting to operate a computer terminal, while in a patrol environment, officers must exercise the utmost care while using the MCT. Officers should not attempt to read the MCT screen or conduct digital commands while the vehicle is in motion.

DCI ACCESS

The MCT affords officers the opportunity to access certain information stored by the North Carolina Division of Criminal Information (DCI), the National Crime Information Center (NCIC), and various state agencies. The limited certification program for MCTs does not allow officers to operate any other DCI terminal.

DCI Log On

Immediately upon logging onto CAD, officers should log onto DCI. The information which officers will be allowed to access through the MCT will be determined by the Chief of Police, upon approval by the DCI Policy Board.

Inquiries

All inquiries made through DCI should be properly formatted and related to official business. Inquiries of a personal nature are specifically prohibited.

COMPUTER-AIDED DISPATCH

The ability of the officer to communicate directly with the telecommunicator through their MCT is often a tactical asset. However, this feature of the MCT is designed to augment, not replace, the police radio.

Call Assignment

Upon receiving a digitally dispatched call, the officer should send an acknowledgment message to CAD by depressing the "ACK" key. High priority calls that are verbally dispatched will also be digitally dispatched and will require the same "ACK" response from the officer. The 10-23 key (arrived on scene) should be depressed upon arrival.

Upon returning to service, officers are responsible for checking their message/call queue and responding appropriately.

Self-Initiated Calls

Any self-initiated call, which is not of an emergency nature, will be initiated by the officer through the appropriate MCT command. The officer will make every effort to include all pertinent information into the entry.

Car to Car Messages

Officers may use the MCT to communicate with other officers and the Emergency Communications Center. The MCT will not totally preempt voice communications. Rules of conduct governing radio transmissions are applicable to any digital messages.

- All car to car messages will be maintained for 90 days.
- Periodic reviews of MCT traffic will be conducted at the direction of the Chief of Police or by personnel in the Office of Professional Standards.