

La Plata Police Department – General Order

	Title: Mobile Data Terminals		Order #: 653	
	Effective Date: November 20, 2014		Review Date:	
	Original Issue:		<input type="radio"/> New <input type="radio"/> Amends <input checked="" type="checkbox"/> Rescinds - Order B.8	
Approved by: Chief Carl Schinner			CALEA 5 th Edition	
CALEA Standard: 41.3.7			Pages: 3	

01 PURPOSE: The purpose of this Order is to define the use of the Mobile Data Terminals (MDT).

02 POLICY: It shall be the policy of the La Plata Police Department to use the MDT to support the Department’s activities. It is the responsibility of each member to ensure that this technology is used for proper business purposes and in a manner that does not compromise confidential, protected, restricted or other sensitive information.

03 MDT COORDINATOR: The Chief of Police will designate an MDT Program Coordinator. The MDT Program Coordinator will conduct random administrative security checks of the MDT system to ensure that all necessary security procedures are being followed. The MDT Program Coordinator will also ensure that required employees are trained on the proper use of the MDT.

04 GENERAL SYSTEM USAGE: (CALEA 41.3.7)

- A. All MDTs, data and software, maintained or used by the La Plata Police Department are for official use only. No employee will use or cause to be used any MDT for personal gain or benefit of any kind.
- B. No employee will attempt to install, delete or modify any software or hardware associated with the MDT without authorization from the MDT Coordinator.
- C. If the equipment needs to be serviced, repaired or reprogrammed, contact the MDT Program Coordinator.

D. For the purpose of this Order the term Mobile Data Terminals is interchangeable with lap top computers with MDT capability.

05 MOBILE DATA TERMINALS (MDTs)

- A. All electronic messaging/correspondence is the property of the Town of La Plata and is assigned to the La Plata Police Department.
- B. Use of Equipment (CALEA 41.3.7):
 - 1. All traffic transmitted using the MDT must be business related and comply with the same quality standards as voice traffic. Offensive, demeaning or disruptive messages are prohibited. Any message containing slang or language that could be construed as a slur, racially biased or sexual harassment against any person or group will not be tolerated. All transmissions are recordable, retrievable and are public record.
 - 2. The only personnel authorized to operate a MDT are those specifically trained in its proper operation. Only those personnel who are METERS (Maryland Electronic Telecommunications & Enforcement Resource System) and NCIC (National Crime Information Center) certified are authorized to access METERS and NCIC.

3. Dissemination of Information: Employees shall treat the official business of the Department as confidential. Information will only be disseminated to those who have an official need to know. Unauthorized request, use, dissemination and/or receipt of LinX or CJIS information may subject the employee to possible disciplinary action up to and including termination/criminal charges and LinX/CJIS/METERS access termination.
4. Employees operating vehicles equipped with the MDTs must remember to give full time and attention to the operation of the vehicle.
5. Employees will keep the MDT screen and keyboard clean using the supplies provided. Food and liquids must be kept away from the MDTs at all times. In the event of an accidental spill, the employee will:
 - a. Log off all active sessions and shut down the MDT as quickly as possible.
 - b. Clean the affected area.
 - c. Notify the MDT Program Coordinator or his/her designee as soon as practical to inspect the unit.
6. When away from the vehicle, employees must ensure that the vehicle is locked to prevent unauthorized use and theft of the MDT.
7. Employee's passwords to access the MDTs and METERS/NCIC shall not be shared or made known to any other individual. Employees who believe that their password has been compromised shall immediately notify the MDT Program Coordinator via memorandum or email and change their password. Attempts by any

employee to utilize a MDT or gain access to METERS/NCIC with another employee's password are prohibited.

8. Hit Procedures:
 - a. Officers receiving a hit on his/her MDT will verify the hit by viewing the NCIC Summary Screen to ensure the hit is for the person or type of property and identical information they requested, prior to initiating a stop, contact or other enforcement activity, unless other probable cause exist for a stop.
 - b. Officers must confirm the hit through the on-duty Communications Specialist prior to making an arrest or recovery.

06 PHYSICAL SECURITY:

- A. Employees are responsible for the MDTs physical security. MDTs will be locked into the MDT stand to ensure security. (CALEA 41.3.7)
- B. Employees are responsible for their assigned NCIC thumb drive. Should a thumb drive be lost or stolen it will be immediately reported through the chain-of-command to the Office of the Chief of Police.

07 SOFTWARE:

- A. Employees may not introduce any software programs or other files into a MDT, desktop or other handheld Department-owned computer without written authorization from the Town's Information Technologies Vendor/Department. (CALEA 41.3.7.a)
- B. Employees will not manipulate or make alterations to current software programs installed on any MDT, desktop or other handheld Department-owned computer. All updating and alterations to programs shall be performed by the Town's

Information Technologies Department.
(CALEA 41.3.7.b)