Georgia Department of Public Safety
Policy Manual

SUBJECT **MOBILE DATA TERMINALS**	POLICY NUMBER **14.05**
DISTRIBUTION **ALL EMPLOYEES**	DATE REVISED **1/26/2011**

14.05.1 PURPOSE

To establish guidelines and regulations governing the safe use of mobile data terminals in DPS vehicles and vehicles utilized by DPS personnel in the performance of their assigned duties.

14.05.2 DEFINITIONS

Mobile Data Terminal (MDT) **-** A vehicle-based computer that provides for dispatching, car-to-car communications, and criminal justice database inquiries.

Member – Any Departmental member (sworn or civilian) who has access to the mobile data terminals.

14.05.3 OBJECTIVE

To increase the efficiency and effectiveness of sworn members assigned to patrol duties.

14.05.4 PROCEDURES

A. Assignment, Security, and Storage of Equipment

1. Assignment of Equipment

a. MDTs will be issued in accordance with DPS inventory control procedures found in Policy #7.10, Inventory.

b. MDTs will be installed in a manner that does not interfere with any occupant restraint devices (air bags and seatbelts). Only authorized personnel shall install or move assigned equipment.

NOTE: Members shall not modify the MDT, the MDT hardware or printers under any circumstance. This includes, but is not limited to, removing parts, adding personally purchased hardware or modifications to any part of the system in general. Members are not to affix any decals or stickers to any component which make up the MDT or printer.

Violations of this directive may result in disciplinary action and may include the requirement to reimburse the Department for any and all damages resulting from such modification(s).

c. Members are responsible for the care and security of each piece of equipment assigned to them or to their assigned vehicle.

   d. Members are accountable for issued MDT equipment and will obtain written receipt for any item returned or exchanged.

2. End-of-Shift Removal and Storage of Equipment

   a. If the member's vehicle will be secured in a locked garage, all MDT equipment may remain in the vehicle.

   b. If a member's vehicle will not be secured in a locked garage, the MDT will be removed from the vehicle and stored in their residence or locked office.

      NOTE: Due to the sensitivity of the equipment to extremes in temperature, MDT equipment shall not be stored in the trunk of an automobile.

3. When the member is on-duty, the MDT will be securely mounted in the available docking device in the vehicle.

4. A member shall not take the MDT on vacation or out of the state, unless they are on official business or are directed to do so by a supervisor.

5. Unattended Vehicles

   a. Vehicles will be locked when left unattended.

   b. Members will use every precaution to safeguard equipment when the equipment is not in their immediate possession.

      1) Members will, if necessary, remove the MDT from the vehicle.

      2) Any MDT that is left in an unattended vehicle must be locked in the docking device and the docking key removed.

   c. The MDT will not be stored in any location that exposes the MDT to extreme heat or cold.

   d. Members will log off of the MDT when it is unattended.

6. Stolen Vehicles and/or MDT

   a. The member's supervisor will be notified immediately if it is believed that an MDT (or a vehicle with an MDT in it) is stolen.

   b. Members assigned MDT equipment will be held responsible for any stolen or missing item if the vehicle is left unlocked when unattended.

   c. Stolen equipment requires the completion of the Lost, Stolen Damaged or Destroyed Property report, DPS-494.

7. Passwords

   a. Members will not give their passwords to any other persons to use nor will they leave the password in any discernible written form on or near the MDT.

   b. In an emergency it may become necessary for a user to share a user-ID and password with another person. In such cases, the user sharing the password has full responsibility for the use of the MDT by the person with whom the user-ID and password have been shared and at the earliest possible time, will change or cause their password to be changed.

B. Restrictions Regarding Access to Criminal Justice Systems

Systems include, but are not limited to: GCIC, NCIC and other confidential law enforcement data information systems.

1. Members **will**:

   a. Restrict dissemination of information received through Confidential Data Systems to authorized criminal justice persons only.

   b. Maintain a criminal history log.

   c. Perform transactions for criminal justice purposes only.

2. Members **will <u>not</u>**:

   a. Access criminal history files except as provided for by law and rule.

   b. Access database records for any reason other than legitimate law enforcement purposes.

   c. Permit use of the MDT by any individual who is not certified for confidential law enforcement data information systems access.

C. Authorized/Unauthorized Use

1. Use of the MDT is restricted to official DPS business. Computer files, including e-mail messaging and GCIC inquiries are subject to review.

2. Use of the MDT by anyone other than authorized members requires authorization from the Communications Adjutant in consultation with the Chief Information Officer.

3. Members are responsible for ensuring the security of the MDT against unauthorized use.

4. If it is believed that unauthorized access has occurred, the member will immediately notify a supervisor.

5. Inappropriate or unauthorized use of the MDT may subject the member to disciplinary action.

D. Software Restrictions

1. DPS Policy #14.02, Computer Security and Crimes, regarding department computers and software are applicable to MDTs.

2. If a member wants additional software loaded onto the MDT, they must submit a written request through the chain of command to the Communications Adjutant. If the Communications Adjutant determines that the additional software is appropriate, he will forward the request to Chief Information Officer. Only software that is business related will be approved. Screen savers, wallpapers, games and other non-business-related software are not to be loaded onto MDT (this does not include software contained on the MDT at the time of purchase).

3. Any unauthorized and/or altered software found on DPS MDTs during maintenance work, upgrades or inspections will be removed and the member may be subject to disciplinary action.

The manipulation or alteration of current software running on-agency owned mobile, desktop or handheld computers is prohibited.

4. Members will not disable or shut off any anti-virus or anti-spyware programs.

E. MDT Operations

1. The MDT will be turned on and the user logged into the SmartMCT Mobile Application on their MDT at all times that a member is operating the vehicle. Members on out of area assignment trips may elect not to leave the MDT on however, will activate and log onto the MDT upon return to their assigned Troop. Members on special assignment in areas that are MDT compatible will have the unit turned on at all times when they are in their car.

2. Members will take care when operating an MDT while driving. Simple inquiries and viewing the nature of an in-coming message may be performed while driving, but extreme caution shall be used. Message response and complex or multiple inquiries **are not** to be conducted while driving.

3. Unless exigent circumstances arise, all members assigned or sharing a MDT shall read and, if required, respond to any email correspondence sent to their assigned account, at least twice during their assigned shift. Checks shall be timed close to the start and the end of the shift. Also, members shall abide by any orders or instructions they receive via email from a supervisor.

4. Foods and beverages are not to be placed on the MDT unit. Care is to be taken to ensure no food, beverage, or other substances are dropped or spilled on any part of the MDT unit.

5. Only members with current GCIC certification are permitted to initiate inquiries into criminal justice databases.

6. Members will not use any other member's login name and/or password to log onto an MDT unit.

7. At all times when MDT usage is required by this policy, the Automatic Vehicle Locator (AVL) function of the MDT shall be used if the MDT is equipped with a Global Positioning Satellite (GPS) unit.

   a. No member shall change any settings or configurations of the MDT software, or make any physical changes to the MDT to cause the GPS to fail to properly report location information to the CAD system.

   b. If the MDT fails to properly report location information to the CAD system, the member shall immediately notify their supervisor, or their designee, of the failure so that appropriate repairs can be made to restore the AVL function.

8. If a member's assignment would be adversely affected by having location information published in the CAD system, the member's Troop Commander may authorize the CAD administrator or the Chief Information Officer to disable the display of location information in the CAD system for as long as necessary to complete the assignment. At the conclusion of the assignment, the AVL function shall be promptly activated to normal operations.