Rockville City Police Department
GENERAL ORDER

Subject **MOBILE DATA COMMUNICATION SYSTEM**		Procedure **G.O. # 4-40**
Authorizing Signature	**Effective** **02-26-10**	**Total Pages** **5**

I. PURPOSE

A. The purpose of the Mobile Data Communications System (MDCS) is to improve the department's responsiveness by utilizing data communications in field units. The MDCS was designed to allow access to federal, state, and local databases. The system also provides a secure method of communication between field units.

B. This policy provides standards and guidelines for the proper and authorized use of the Mobile Data Computer (MDC) by department members as a means of communicating (e.g., dispatching calls for service, access to CAD, etc.) with ECC and other members, maintaining the status of field units, and conducting field reporting. This policy applies equally to all department members unless the context or specific language indicates limited applicability.

II. GENERAL PROVISIONS

A. All users with a fixed mounted MDC will immediately activate and log onto their MDCs when operating their police vehicle. All other users are encouraged to log on in order to enhance safety and emergency responsiveness.

B. Supervisors will periodically check to ensure employees remain signed on as required by this directive.

C. Subject to section II.D, all users are encouraged to use the MILES/NCIC query functions to identify wanted or missing subjects and stolen vehicles and property when not running calls for service or engaged in other departmental activities.

D. Safe Use

The driver of any vehicle equipped with an MDC shall always attempt to use the MDC in a safe manner. Safety of the officer, other vehicles, and tactical operations takes a priority over any mobile data operation.

E. Hit Procedures

1. Officers receiving a hit on their MDC 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 or contact.

2. Officers must confirm the hit through communications prior to making an arrest or recovery.

F. Packet Cluster Patrol (PCP) Talk Groups

All users will sign onto a PCP talk group that correlates to their CAD dispatch group. Police supervisors are reminded that keeping their units on the talk group assigned to their CAD dispatch group will ensure that their officers are able to view all activities occurring within a district.

G. Providing a Clearance

Officers assigned as the primary officer on a call will be responsible for providing the clearance.

H. Voice Communications

While officers are expected to use the MDC as much as possible to reduce airtime, voice communications will be used whenever it is deemed necessary for officer safety reasons.

III. ELECTRONIC MESSAGING PROCEDURES

A. All electronic messages should be considered in the public domain. Employees should have no expectation of privacy regarding electronic messages. All transactions on the MDC are electronically logged. All electronic messages should be professional. To assure proper procedures are being followed, supervisors may request to periodically review message logs.

B. Any electronic message that is sent through the MDC system may later be retrieved by authorized personnel, even though it may have been deleted from the assigned employee's MDC. Electronic messages are not a protected form of communication and could be subject to a discovery motion in a criminal case, civil case, or internal investigation.

C. Broadcast messages to all system users must have the prior approval of a supervisor or concern an operational law enforcement matter that precludes prior approval.

IV. SECURITY

A. Physical Security

Officers will be responsible for the MDC's physical security, whether in or out of the vehicle and for obtaining any required maintenance through the Mobile Data Help Desk and the Montgomery County Police Technology Division. An officer who is assigned a bag unit MDC will not leave it in the passenger area of the vehicle when the vehicle is unattended for a long period of time (i.e., parked at the officer's residence overnight). When a mounted MDC is left in a vehicle, it must be locked in the docking station and the key must be removed and secured.

B. Authorized Users

Use of a department MDC by anyone other than an authorized user is prohibited. Only the following are authorized to use the MDC's:

1. Employees that have attended mobile data training and have a valid user name.

2. Field training participants.

C. Passwords and Changes

Access to the MDCS will be controlled through assigned logons. Employees will be provided passwords during training. Employees may change their passwords at any time. Employees will make every effort to keep their password private. Employees will not give their passwords to any other person nor will they leave the passwords in any discernible written form in or near their MDC. Users are required to change their passwords as prompted by the system.

D. Notification

Departmental personnel must immediately notify their supervisor and the Technology Division if an MDC or peripheral equipment is damaged, stolen, or it is believed unauthorized access was attempted or gained. Department procedures for reporting damaged/stolen equipment will be followed.

V. SYSTEM MODIFICATIONS

Hardware and software modifications or changes to the mounting system are prohibited except when authorized by the Montgomery County Police Technology Division Director. Only software tested and approved for the MDCS can be installed on MDCs. Employees who wish to use other software must submit the software to the Montgomery County Police Technology Division for configuration testing and approval prior to installation.

VI. MAINTENANCE

A. The Montgomery County Police Technology Division is responsible for maintenance, support, and repair of the MDC software. Requests for service should be routed through the Help Desk at 240-777-5219. Technology Division personnel will be available 24/7 for calls about mobile data problems. If required, they will respond to the user and arrange for a service time or replace the computer. Officers experiencing problems with hardware or software should first contact a mentor. Hardware problems should be brought to the attention of the department's PS2000 liaison.

B. Mentors

Mentors are specifically trained officers who can assist with minor hardware or software questions. Mentors can be reached at each station. If a mentor is not available, the officer should call the Help Desk for assistance. Mentors will not be called back on overtime for mobile data related problems. The mentor list is available in the CAD and will be maintained by all station PDSAs.

C. Help Desk

The Help Desk, at 240-777-5219, is an automated service that will let the officer know of known service outages and problems. From the menu, the officer can select the MCPD Help Desk feature. The line provides access to help with password, hardware, and software problems. If problems cannot be resolved on the phone, additional personal Technology Division help is available.

D. Passwords

If a user has problems with or has forgotten their MILES password, contact the department's mobile data security officer. If unavailable to contact him/her, then contact the Help Desk at 240-777-5219.

VII. TRAINING

A. All users of the MDCS must attend a PS2000 mobile data class and must maintain current certification for MILES/NCIC.

B. All training will be performed by Montgomery County Police Department approved instructors.

VIII. DISPATCHING

A. The ECC dispatcher will voice dispatch all information for calls with a priority of 0 to 7 but will only dispatch the nature and location for calls with priorities 8 and 9. For those calls, officers will be responsible for obtaining the information off of the MDC.

B. Acknowledgement

1. Whenever possible, officers will place themselves "enroute" to a call using their MDC.

2. When a unit fails to acknowledge a call either by voice or MDC, and the dispatcher is unable to make radio contact with an officer after three attempts, the dispatcher will advise the officer's supervisor and announce a lookout for the officer on the primary channel. If the officer's supervisor is not available, any off-duty district supervisor will be notified. The dispatcher will also notify the ECC supervisor of the lookout.

The patrol supervisor will take appropriate action to locate the missing officer and cancel the lookout when the unit is accounted for.

3. Officers will use their MDC to access MILES/NCIC data unless doing so would compromise officer safety.

4. Off-duty officers may, but are not required to, log onto the MDC with a status of "off duty". Off-duty officers will be responsible for answering calls as in accordance with General Order 4-39, Personal Patrol Vehicles.

5. Off-duty officers will log off the system prior to leaving their vehicles for extended periods of time.

IX. AUTOMATIC VEHICLE LOCATOR

The Automatic Vehicle Locator (AVL) is a system, which allows ECC to identify the location of vehicles that have been equipped with fixed mounted computers. Intermittent signals are sent to ECC to provide location data as needed. This is a critical officer safety tool. AVL data will not:

A. Be stored, retained, or recorded in any manner.

B. Be used in or for any investigation whether criminal, civil, or internal.

C. Be used in any proceeding that could result in discipline, to include but not limited to internal affairs proceedings.