Mobile Data Computers

.01 Policy

It is the policy of the Bladensburg Police Department to deploy mobile data computers (MDC) as a tool to enhance communications for law enforcement activities such as incident management. It also provides a mobile interface to the Maryland Integrated Law Enforcement System (MILES) and, FBI's National Crime Information Center (NCIC), National Law enforcement telecommunications System (NLETS), and Maryland Motor Vehicle Administration (MVA) databases.

.02 Terms

Mobile Data Computer: Mobile computing devices equipped with wireless or wired communication capability.

.03 Governing Legislation and Reference

Governing Legislation:

Electronic Communications Privacy Act.

Maryland Code, Criminal Procedures Article, §7-202, §8-606, and §10-213 through §10-228.

COMAR 12.15.01.15.

Forms:

CJIS Operator Certification and Logon ID Application.

Criminal Record Request Log (Form #609).

.04 Procedure

Officers will not use the mobile data computer (MDC) until they have received MDC training and MILES/NCIC certification.

Only software purchased or acquired by the Town will be installed on the MDCs. The IT Manager will approve all software installation or repair.

Employees will not modify any computer equipment or install any device or program, including but not limited to any peripherals such as external storage devices, printers, scanners or any type of communication device without written approval of the Chief of Police.

Special care will be taken to prevent the spillage of liquids onto the MDC.

All MDC transmissions are recorded and are recoverable. Abusive, profane, demeaning, harassing, or threatening messages are prohibited.

Employees will adhere to all federal and state law and department policy and procedures.

Criminal justice information will not be disclosed to any unauthorized person. Criminal history (CHRI) will not be disseminated to anyone other than authorized law enforcement personnel. Care will be taken to shield the MDC screen from civilians or arrestees.

Employees will create a Criminal History Request Log entry when receiving a positive criminal history record information (CHRI) query. The Criminal History Request Log is maintained in communications.

Trained officers operating a police vehicle equipped with an MDC will log-on to the system while in service. Officers will log-off and shut down the MDC if they expect to be away from the vehicle for more than thirty minutes.

Safe vehicle operation is of primary concern when using the MDC. Officers will stop their vehicle before using the MDC if use is going to divert attention from the safe operation of the vehicle. Generally, it is not appropriate for officers to operate the MDC while their vehicles are in motion.

When officers receive a warrant hit, they will confirm the warrant with communications over the police radio prior to prisoner transport.

When officers make a traffic stop or investigate a suspicious vehicle, they will use the police radio to notify the dispatcher of their status and location. Traffic stops will also be cleared via police radio.

Mobile Data Computers

Inspections

At least monthly, a supervisor will inspect MDC's. If any deficiencies are noted, the supervisor report the nature of the deficiency by email to the Commander of Operations.

Security

Employees must take steps to protect assets, such as mobile computing devices, from loss or theft and to protect restricted data that may reside in such devices from unauthorized access.

Employees will not leave the MDC or data storage devices in an unsecured unattended vehicle, even for a short period of time.

Off-duty officers will remove the MDC and data storage devices from the vehicle and store them in a their residence or locked office.

HISTORY: Adopted May 16, 2008

This General Order supersedes all other orders and memoranda in conflict therewith.

Authority:

Charles L. Owens
Chief of Police