GENERAL ORDER

METROPOLITAN POLICE

DISTRICT OF COLUMBIA

Title	
Use and Operation of Mobile Data Computers	
Number	
GO-SPT-302.09	
Effective Date	
March 21, 2012	
Replaces: GO-SPT-302.09 (Use and Operation of Mobile Data Computers), Effective Date April 2, 2009 **Rescinds:** GOC-11-05 [(GO-SPT-302.09 Use and Operation of Mobile Data Computers)], Effective Date November 2, 2011 TT 02-009-12 (Vehicle Computers & Mount Repair Process), dated May 16, 2012	

I. BACKGROUND

Mobile data computers permit members in the field to access the Metropolitan Police Department (MPD) main computer and the WALES (Washington Area Law Enforcement System) and NCIC (National Crime Information Center) databases. This access saves time in relaying information, improves police response time, and ensures members are provided accurate information because the information is available for frequent reviews. In large incidents, members can use the mobile data computers to communicate with one another with vehicle-to-vehicle transmissions and with members of other law enforcement agencies without excessive use of the radio.

II. POLICY

It is the policy of the Metropolitan Police Department to ensure that mobile data computers are used properly by members to improve police service within the District of Columbia.

III.   DEFINITIONS

When used in this directive, the following term(s) shall have the meanings designated:

1.   Member - Sworn or civilian MPD employee or MPD Reserve Corps member.

2   Mobile Data Computer (MDC) - Terminal that permits members to communicate directly with remote computers and crime information databases and to communicate vehicle-to-vehicle without using a police radio.

IV.   REGULATIONS

A.   MDCs shall be considered mobile radios and subject to the requirements of General Order 302.05 (Radio Communications).

B.   MDCs are MPD property and shall be used only for official police business.

C.   MDCs shall be used only by authorized MPD members who have been trained and certified to use them.

D.   MDCs interface with law enforcement information systems, including WALES and NCIC, and shall be used only by those individuals trained and authorized to access these systems.

E.   Under no circumstances shall any member use an MDC to access a restricted law enforcement information system, including, but not limited to, WALES and NCIC for personal reasons. Any accessed information shall be used for only law enforcement purposes.

F.   Members using MDCs shall comply with General Order 302.6 [The Washington Area Law Enforcement System (WALES)].

G.   Vehicle-to-vehicle messaging shall be used to reduce voice radio traffic.

1.   Members shall recognize that MDCs are not intended to replace telephones or be a casual means of communication. MDC recordings are provided to agencies outside the MPD for investigative purposes and are subject to subpoena.

2.   All MDC messages shall be professional and job-related.

a.   Members shall not use harsh, violent, coarse, profane, sarcastic, or prejudicial language; or

        b.   Use terms or words that might be interpreted as derogatory, disrespectful, or offensive to the dignity of any person.

H.   Members shall not install unauthorized software on any MDC.

I.   Members shall not willfully damage or permit any MDC to be damaged.

J.   Members shall not allow unauthorized persons to tamper with, or operate, any MDC.

K.   Members are responsible for all system transmissions sent under their user ID.

L.   Members are prohibited from using any other member's user ID and password.

M.   Members shall safeguard their user ID and password to prevent access by others.

N.   MDC-equipped vehicles may be jump started, and may be used to jump start other vehicles, but only after the MDC operator(s) has logged off and turned off the power to the MDC.

O.   Members shall not remove or transfer a MDC from one vehicle to another.

P.   If the MDC is missing from its assigned vehicle or unlocked in the docking station, members shall:

        1.   Immediately notify an official and the Vehicle Maintenance Officer (VMO).

        2.   Prepare a PD Form 43 (Report of Damage to or Loss of District Government Property).

        3.   Document the missing or unlocked MDC on a PD Form 775 (Daily Vehicle and Inspection Report).

Q.   See GO-SPT-302.11 (Telecommunication Devices) for procedures regarding the purchase of laptops/MDCs with grant funding.

V.   PROCEDURES

A.   Logging In and Maintaining Status for MDC in Vehicles

        1.   Members assigned to a vehicle with an MDC and docking station shall complete a thorough inspection of both the computer and mount, to include all bolts, wires, and connections. The appropriate entries related to the inspection shall then be made on the PD Form 775.

        2.   Members shall perform a login for that MDC (10-99 or 10-4) provided the member has a login code.

        3.   If any damage or inoperability is found with the MDC and/or associated equipment, members shall notify an official of their assigned unit,

record the name and badge number of the official on the PD Form 775, and prepare the appropriate documentation for the damage [for example, PD Form 251 (Incident-Based Event Report) and PD Form 43 (Report of Damage to or Loss of District Government Property)].

4. Members shall come into service (10-99 or 10-4) with a communications operator at the Office of Unified Communications (OUC) at the beginning of their shift as soon as practical after starting their vehicle and inform the OUC operator whether the assigned vehicle is MDC-equipped and if the MDC is operational.

5. Members shall remain logged on to the MDC at all times for the entire shift.

    a. Members shall ensure that their current and correct status is provided at all times.

    b. The operator of the police vehicle shall not type messages or entries while the vehicle is in motion.

    c. When stopping a vehicle or suspect, member(s) shall immediately notify an OUC communications operator of the stop location as well as the stopped vehicle's tag number.

B. Crime Data Information Databases Queries and Hits for MDC in Vehicles

    1. Members shall use an MDC to make their own WALES and NCIC queries unless circumstances render such queries unsafe or impractical and subject to the requirement in Part V.A.5.b of this order.

    2. A member who receives a positive MDC return indicating a WANTED person or vehicle shall immediately re-notify an OUC communications operator of the location of the stopped vehicle and advise the operator of the "Hit" by using the term "10-3-0" (ten-three-zero).

        a. The OUC communications operator shall immediately send the closest available unit to respond to the stop location to provide back-up for the member whose check resulted in a "Hit."

        b. Once the suspect is in custody and, upon leaving the scene of the arrest, the member shall notify the dispatcher of the change in location and whether a Central Complaint Number (CCN) will be needed.

        c. If a member receives a WALES return indicating an invalid permit status that necessitates an arrest, the member shall advise an OUC communications operator to send another unit to the scene of the stop for a "10-3-0" (ten-three-zero) to stand by with the prisoner while the prisoner's vehicle is secured.

d.   The MDC operator shall ensure that the suspect is, in fact, the wanted person described in any WALES/NCIC return and shall review the NCIC Soundex returns received over the MDC.

C.   Vehicle-to-Vehicle Messaging

1.   As required by Part V.A.5.b of this order, operators of police vehicles shall not type any MDC message or make any MDC entry while the vehicle is in motion.

2.   Members shall transmit all messages in English, except when the prior approval of a supervisor has been obtained to communicate in a language other than English.

D.   Logging Off of MDC in Vehicles

1.   Members shall log off the PacketCluster patrol system and the CAD system at the end of their shift and whenever the MDC will be left unattended for an extended period of time (for example, for attending court or training).

2.   Members shall secure the vehicle (i.e., lock the doors and trunk) to prevent theft or unauthorized use of and/or tampering with an MDC.

E.   Maintenance and Repair

1.   Members shall be responsible for ensuring that the MDCs are kept clean and dry.

2.   Members shall use only cleaning products designed for cleaning electronic equipment.

3.   Members shall not place food and beverages around the MDC equipment.

4.   Members shall not place any object on the top of an MDC or MDC docking station.

5.   Members shall keep the area of the vehicle's trunk occupied by the MDC electronic equipment as clear as possible (i.e., required equipment only).

6.   When entering an automatic car wash, members shall first turn off the Sierra Wireless modem. Users with a two (2) piece cellular digital packet data (CDPD) antenna shall remove the top half.

7.   When members experience any problems with an MDC in a vehicle or its docking station, the member shall notify their immediate supervisor.

   a.   Upon the supervisor's approval, member shall contact the MPD Help Desk at 202-727-3302 and provide the following information:

      (1)   Vehicle tag number;

      (2)   Cruiser number;

      (3)   Valid call back number;

      (4)   District watch commander's number (to coordinate the vehicle's availability for repairs); and

      (5)   Detailed description of the issue.

   b.   The reporting member shall:

      (1)   Record and log the remedy ticket number provided by the MPD Help Desk staff.

      (2)   Provide the watch commander and if available, the district vehicle maintenance officer (VMO) with the remedy ticket number.

8.   Members who, at any time during a shift, find the MDC in a vehicle and/or associated equipment to be damaged or inoperable shall immediately report these circumstances to an official and follow the procedures contained in this order to include completing a PD Form 43.
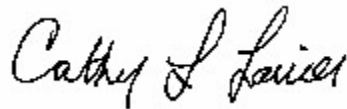
VI.   ROLES AND RESPONSIBILITIES

A.   Members shall be responsible for:

   1.   The care, safekeeping, and proper use of the assigned MDC during the assigned shift.

   2.   Reporting inoperability and damage in accordance with Part V.E.7 of this order.

B.   Watch Commanders shall:

1. During each shift, assign an official to ensure that vehicle-MDCs and/or its associated equipment are inspected, operational, and not damaged. The designated official shall:

   a. Report any inoperability/damage to the Watch Commander for that shift.

   b. When possible, report the cause of the damage (i.e., accidental, intentional, or normal wear and tear).

   c. Prepare the appropriate documentation (for example, PD Forms 251 and 43).

2. Record on the PD Form 150 (Tour of Duty Supervisor's Report) the status of each vehicle-MDC being operated on his/her watch and attach any related PD Forms 251 and 43 for damage to the Report; and

3. Notify immediately the VMO of any damage to a vehicle-MDC and/or its associated equipment that has been found to report the damage in accordance with this order.

C. VMOs shall:

1. Secure the MDC when a vehicle is sent to the shop for a non-MDC issue (e.g., repairs, 10-50, or damage).

2. Ensure that damaged MDCs and/or associated equipment are repaired as soon as possible.

3. Track and monitor the MDC's and/or the associated equipment's repair status.

4. Notify the watch commander when repairs are complete.

D. Commanding Officials shall ensure:

1. Assigned personnel are properly trained in the use of MDCs.

2. MDC-equipped vehicles are inspected biweekly.

   a. The inspection shall include a visual and physical examination of the MDC hardware and software in each patrol vehicle.

   b. The results of the inspection shall be included on the PD Form 775-A (Weekly Vehicle Inspection Checklist) for the vehicle in which the MDC is installed.

E. The MPD-Office of the Chief Technology Officer shall be responsible for the overall implementation, control, and maintenance of the mobile data computer system and shall ensure that for reported problems the MPD Help Desk:

1. Opens a remedy ticket.

      2.   Provides the remedy ticket information to the reporting member.

      3.   Forwards the request for service to the correct vendor.

F.   The Office of Risk Management shall conduct periodic audits of vehicle-to-vehicle message transmissions.

VII.   CROSS REFERENCES

A.   General Order 302.05 (Radio Communications)

B.   General Order 302.06 [The Washington Area Law Enforcement System (WALES)]

Cathy L. Lanier
Chief of Police

CLL:PAB:MOC:JC