Colorado Springs Police Department

General Order

1510 Mobile Computer Procedures

Section 1500 – Assigned Equipment

Effective Date: 1/24/2022
Supersedes Date: 2/17/2021

.01 Purpose

The purpose of this directive is to provide direction on the use and expectations for using the department's mobile data computers (MDC).

.02 Cross-Reference

GO 1063 Communications Protocols
GO 1612 Records Security
DL-1020-01 Crimes in Progress
DL-1510-01 Car-to-Car Messaging

.03 Discussion

In the interest of efficiency and in the effective delivery of services, department personnel who routinely conduct field work will be assigned an MDC or have one made available to them for official department use.

.04 Policy

Under no circumstance will any directive outlined in this policy be intended to compromise personal safety.

.05 Definitions

Mobile Data Computers (MDC): a laptop issued by the department or assigned to department personnel for use in the field.

.10 Use of MDC by Police Personnel

The department has provided MDCs for use by personnel who conduct fieldwork. Personnel who have been issued or have otherwise had an MDC afforded to them will go in service with a functioning laptop. If the laptop is found to be out of order, a request for maintenance will be initiated, following the procedure outlined in this order.

While certain pieces of information are required to be broadcast using a police radio, the MDC can be used in a number of situations.

.12 Clearing Calls for Service

Personnel will clear themselves from each call for service using the MDC unless personnel feel it is necessary to air hazards, BOLOs, or other necessary information.

.14 Wants/Warrants Checks

Personnel will use an MDC to make all CJIS/CCIC/NCIC inquiries and confirmations unless circumstances exist that make using the MDC impractical (e.g., away from the MDC and unable to leave a location or unable to return to the car to use the MDC).

Officers will verbally notify dispatch of contact with any party determined to have wants/warrants using the MDC.

.16 Log Off Protocols

All personnel are required to log off from an MDC and to disconnect from all network computer systems at the completion of their workday.

.20 Digital Dispatching

While calls for service will primarily be dispatched, some may be digitally (non-voice) dispatched (e.g., responses to property crimes in which an unknown suspect is unlikely to have remained on scene after the crime). These standards may be overridden at any time if personnel determine a need to disregard the standards (e.g., personnel requesting assistance/emergency response).

.22 Requests for Emergency Assistance

Personnel will not request emergency assistance using the MDC, whenever practical.

.30 Use While Driving Prohibited

The driver of any vehicle will not manipulate/use an MDC while the vehicle is in motion. If necessary, personnel will make every effort to stop their vehicle and park, in a safe manner, before attempting to access information on the MDC.

Personnel found to have been using their MDC during a traffic crash may be subject to discipline.

.32 Use for Official Business

Personnel will only use an MDC for official department business. Personnel will not use an MDC or allow others to use their MDCs to conduct inquiries of law enforcement databases that are not for official business.

.34 Unauthorized Access

Use of a department MDC by anyone other than an authorized user is prohibited.

Personnel who believe an assigned MDC may have been used or was attempted to be used for unauthorized access to the department's/city's network will immediately report the situation to the city's IT section.

.40 MDC Assignments

All officers, corporals, and sergeants in the patrol division are assigned MDC computers. All personnel utilizing MDCs are required to remove their personally assigned MDC from the vehicle at the end of each shift and store it securely.

.42 MDC Troubleshooting

Personnel who experience problems with a department MDC will contact their divisional tech team officer so as to allow the tech team officer the opportunity to troubleshoot potential issues.

If the divisional tech team officer is unable to resolve the issue, the tech team officer will contact the city's IT section for all maintenance, support, repair and/or replacement of department computers. The tech team officer will complete the Technology Tracking form and submit it to the technology team supervisor. The technology team supervisor will make the appropriate changes in Quartermaster for asset tracking purposes.

.44 Damages to MDC After Business Hours

If an MDC is damaged and/or becomes inoperable after business hours, the personnel will contact a supervisor to issue a spare laptop.

The supervisor receiving such notification will notify their divisional tech team officer of the nature of the problem and the assigned officer's information (e.g., name, IBM, shift). The supervisor will also provide the tech team officer with the spare MDC information (e.g., computer name, serial number, and IMEI number) for tracking purposes.

Damaged MDCs will be immediately reported to the city's IT section by the assigned personnel.

Any exceptions to the above protocol must be authorized by a supervisor or the duty lieutenant.

.46 Spare MDC

Each division has a number of spare MDCs that are available for the immediate replacement of damaged laptops, as well as for extra duty assignments that require the use of a computer (e.g., Walmart).

The division commander, or their designee, will be responsible for ensuring spare MDCs are accounted for and are available for any required maintenance through the department's technology section.

If an employee requires the use of a spare MDC, the supervisor will assign the device to the employee in QoQ. In the event the supervisor is not properly trained in QoQ, they will notify the equipment sergeant who will reassign the MDC in QoQ. Spare MDCs will be signed out to a specific officer in accordance with procedures established for QoQ.

The spare MDC will be returned to divisional inventory immediately upon return of the repaired unit. Employees will have a supervisor sign the spare back in by using the QoQ system. If a spare MDC will be permanently assigned to the employee, the proper comment should be added to the QoQ system.

.47 MDC Inspections

Officers checking out spare MDCs will perform a three-point inspection at the time of checkout, and the individual accepting a returned MDC will perform the same inspection prior to accepting it.

The MDC three-point inspection (function test) consists of:

1. Inspect exterior casing: Check terminal plugs looking for melted portions and other casing deformities.
2. Interior casing: Open the MDC. Check the screen hinges and the inside casing for melted portions, cracks, and other deformities.
3. Inspect functionality: Power up the MDC on battery and ensure you have a visual screen display.

Supervisors will initiate appropriate remedial or disciplinary action for damage caused intentionally or by gross negligence.

.48 Extra Duty Assignments

Officers who have been assigned an MDC are expected to use their issued laptop for extra duty assignments.

.50 MDC Storage and Security

Personnel who are assigned or are otherwise afforded the use of an MDC (e.g., CSO, teleworking personnel, etc.) will be responsible for the device's storage and security (e.g., locking a vehicle when left unattended, securing the device in a locked location when not in use, etc.).

Stolen MDCs will be immediately reported to the city's IT section by the assigned personnel.

.52 External Storage Media Storage and Security

Personnel who use any form of external storage devices with their department MDC (e.g., USB flash drives, external hard drives, etc.), are responsible for safeguarding the device and information stored within the device.

All department directives regarding records and information security apply to all external storage media.

.60 Training

Personnel who are authorized to access law enforcement/criminal justice records or systems will maintain an Operator Security Number (OSN).

It will be the responsibility of the CSPD Training Academy to design and administer additional computer training specific to the software available to the assigned employee.