	Alexandria Police Department Directive 3.3	

MOBILE COMPUTERS

Effective Date: 08-03-2020	**Cancels**: 01-07-2009	
Updated Date:	**Section(s):**	**SME Review Date:**
Updated Date:	**Section(s):**	**2024**
Updated Date:	**Section(s):**	

CONTENTS

3.3.01 PURPOSE AND POLICY

The purpose of this directive is to establish guidelines for the use of mobile computers. Unless otherwise noted in this directive, requirements and procedures for report completion remain unchanged.

It is the policy of this Department to develop and provide the most effective, efficient, and reliable technology to all members of the Department, to provide increased efficiency in communications, report writing, and other automated tasks through mobile computers.

3.3.02 DEFINITIONS

GPS: Global Positioning Satellite- a method of receiving radio signals from satellites in space and triangulating to determine the device location. Accuracy ranges from 10-100 yards.

Mailbox: An electronic holding area in a *server within the records management system* where reports awaiting completion or approval are stored. Each user of the reporting software has a mailbox.

Mobile Computer: The hardware device, usually a laptop computer*, tablet, or cellphone*, which is used by officers in the field to run communications, report writing, NCIC/VCIN inquiries, and other software applications.

NCIC: National Criminal Information Center

TCS System Administrators: Members of the Tactical Computer Section (TCS) responsible for hardware and software configuration and maintenance.

VCIN: Virginia Criminal Information Network

Vehicle Mount: A system of hardware and brackets used to hold the computer in the vehicle.

3.3.03 TRAINING AND SECURITY

A. Only officers who have been trained to use the mobile computers will use them. TCS will maintain a list of trained officers.

B. TCS will ensure that several officers throughout the department are trained as instructors for the specialized software on the mobile computers.

C. Officers using mobile computers must attain a minimum of VCIN *Limited Access Level* certification prior to accessing the VCIN queries. Information obtained through VCIN/NCIC is for criminal justice use only and may not be disseminated or provided to non-criminal justice personnel, unless otherwise prescribed by law.

D. Officers will ensure that no unauthorized person can view information on the mobile computer screen. **[82.1.1.a]**

E. Officers will ensure that the mobile computer is only used in a secure area, such as in a police vehicle or under the officer's immediate control if used outside of the police vehicle. If left unattended while on-duty, the mobile computer must be locked in a secure location such as a locked police vehicle *and on-screen data must be hidden from view*.

F. Officers are reminded that <u>all</u> information sent over the mobile computers is recorded and can be retrieved for review.

G. Passwords

1. The TCS system administrator will *facilitate the issuance of* a password to each user for each software program that requires one. Users *will* choose their own passwords. Officers will contact a TCS system administrator to *reset* or change passwords *if necessary*.

2. Passwords are confidential and may not be shared or disclosed.

3. Officers will only use the password(s) assigned to them and may not use the password of another officer.

4. Officers who believe that their password may have been discovered or used by another person will advise a TCS system administrator of the breach of security and *change their password or* request that a password *reset* be *facilitated*.

H. If a mobile computer is lost or stolen, a TCS administrator will be contacted immediately in person, by phone or by *email*, in order to disable the wireless communications.

3.3.04 CARE OF MOBILE COMPUTERS

A. Employees are responsible for the use and care of the mobile computers in their possession and may be held administratively and financially liable in the event of loss or damage, as with other Department property.

1. Mobile computers needing repair will be left in a location designated by TCS staff. A TCS repair request will be completed and left with the computer.

2. Users will promptly report in a police report and prior to the end of the shift, any damage to mobile computers or vehicle mounts, with the exception of normal wear and tear. *The* police report *case number* will be forwarded to TCS. If there is any question as to whether the damage must be reported, consult a TCS staff member.

B. Employees will not place drinks, food, or other items directly on the computer, or in a location that may cause a spill onto the computer.

C. Officers may use external media such as flash drives or memory cards to store documents and files created by them on the mobile computers. TCS will assist the officer with transferring files from the hard drive if necessary. It is the user's responsibility to notify TCS of files that need recovery.

D. Officers are encouraged to use the mobile computer and software it contains for any departmental or law enforcement purpose.

E. Only TCS staff or other authorized personnel may add, delete or modify the software on the mobile computers. **[41.3.7]**

F. TCS staff will conduct an annual inventory and maintenance of the mobile computers.

G. **Storage:**

1. Computers assigned to individual officers may be stored in the officers' assigned cruiser or another secure location when not in use.

2. Computers left in vehicles overnight must be locked into the locking system provided.

3. Mobile computers in need of repair will be left in a location designated by TCS staff.

4. Mobile computers will not be left in the vehicle when the vehicle is left at the City shop or other repair facility.

H. Inclement Weather:

Computers will not be placed on the floorboards of the police cruisers during rainy or snowy weather due to the chance of water intrusion into the internal components of the device.

3.3.05 DATA COMMUNICATIONS PROCEDURES

A. If available, the mobile computer will be used for the routine communication of:

1. Marking in and out of service.

2. Messages.

3. Status Changes.

4. Mark en-route and on-scene.

5. Changing the officer's location.

6. Clearing calls; backup officers will mark "available," and the officer clearing the call will use the appropriate disposition, along with any comments necessary. Officers will use the comments area whenever possible to document information about the disposition or any actions taken during the call.

7. Other information between dispatchers and officers.

B. By using the mobile computer, the radio is kept clear for emergency traffic. This does not preclude officers or dispatchers from using the radio during emergencies or for officer safety reasons, or when officers are away from their vehicles.

C. *Officers have the option to use either the radio or their MDBs to mark out on traffic stops. When available DECC will verbally announce all traffic stop locations when an officer marks out on MDB.* Officers on special assignments, such as DWI details, may use the mobile computer for traffic stops with prior approval from the dispatcher assigned to the detail. Officers on a traffic stop will mark "available" at the conclusion of the stop, unless a case number is requested, at which time the stop will be cleared with a disposition. Officers should confirm their status with the dispatcher when *radio traffic is clear for routine communication*.

D. Officers will not dispatch themselves to calls or respond to calls to which they were not dispatched and will take all call assignments from the dispatcher. (See Directive 10.29, Radio Communications, section 10.29.03.B.)

E. Patrol and other officers required to remain available for calls will not change their status from available to busy without approval from the dispatcher. Off duty officers may select the appropriate busy status for their detail: extra duty for private employers and off-duty for city paid details. Officers already dispatched on a call or assignment may also, without dispatcher approval, change their busy status to give updates on location changes or other information. Officers not required to remain available for calls may use the busy status to update their location and activity as needed.

F. Information sent over the car-to-car messaging section should be limited to short messages that are appropriate in nature. They are considered official correspondence and shall be handled with the same degree of propriety. Every electronic transmission should be considered in the public domain and shall be professional and courteous.

Messages may be retrieved by authorized personnel at a later time, even though they may have been deleted. Electronic messages and e-mail are not a protected form of communication and could be subject to a discovery motion in a criminal case, civil case, or internal investigation.

G. Officers will promptly report any problems with the mobile computer hardware or software to a TCS system administrator and may be required to complete a repair request form.

H. Officers will report any problems with mobile computers relating to communications personnel or communications procedures through their supervisor to a communications supervisor.

I. When an officer experiences an error or malfunction during the transmission of a message to communications, the officer should contact communications by radio or other means to confirm that Communications received the message and has their correct unit status.

J. Communications personnel will give a radio broadcast when a malfunction in CAD or other systems causes the communications to the mobile computers to go offline. A broadcast will also be sent once the system is back online. Any instructions for restoring connection to the system will also be broadcast by radio.

K. Data will be stored for a minimum of *three* years.

1. Criminal investigation queries will be requested through TCS.

2. Supervisors may use system tools available to them for routine query and auditing of officer activity.

3. *Office of External Affairs and Professional Responsibility* queries *and other internal queries* will be requested through *OPR.*

3.3.06 COMPUTERIZED REPORT WRITING

A. <u>Officers</u>

1. Unless otherwise directed by the watch commander, officers will complete all accident reports (FR300s), incident reports, and field contacts using the computerized report software.

2. Officers are prohibited from signing or approving the report in the supervisor's section unless they have approving authority.

3. After *completing* the report, the officer will electronically transmit the report to the appropriate supervisor's or approving authority's mailbox for review and approval.

4. Officers will then notify their supervisor by sending a message via the computer, by advising them over the radio, or by other means, that they have sent a report to the supervisor's mailbox.

5. Officers will ensure that completed reports are sent to an on-duty supervisor for review.

B. Supervisors

1. Supervisors will check their mailbox throughout the shift and at the end of their shift for any reports awaiting approval.

2. Supervisors will electronically retrieve reports awaiting approval from their mailbox and review and approve the reports using the computerized report software.

3. After reviewing the report, the supervisor will electronically sign and approve the report.

4. *Upon supervisory approval, the report will be transmitted* for final submission to the records management system.

5. If a supervisor finds a mistake in a report, a note describing the correction required will be typed in the administrative notes field, located in the supervisor sign-off section. The report will then be electronically transmitted back to the officer's mailbox. The officer will retrieve the report from their mailbox, correct the problem and then send it back to the supervisor's mailbox for approval.

6. After a report has been transmitted for final submission to the records management system, the master report is not to be retrieved for any changes. Any corrections will have to be made through the records supervisor or by completing a supplemental report.

3.3.07 MOBILE MAPPING

A. Mobile Mapping provides advanced mapping tools. The primary purpose of this mapping system is to provide real time geographic information to communications staff, officers, and commanders**.**

B. Computers equipped with GPS devices and associated software will display on the map.

1. Other data, such as calls for service and links to further information will also display on the map.

2. Employees may not alter the equipment or software to disable the mapping features, with the following exceptions:

   a. Special investigative units may turn off the GPS software in order to safely accomplish their mission and avoid compromising investigations.

   b. Commanders may allow officers or supervisors to temporarily turn off the GPS software for a short period of time in order to accomplish an investigation or special assignment.

3. Data from the systems will be stored in accordance with section 3.3.05.K., of this directive.

4. The GPS system is based on wireless radio signals from satellites.

    a. The locations and data associated with these signals are accurate only for general tactical reference - 10-100 yards average.

    b. A computer that loses connection to the data network will not be able to transmit GPS information.

    c. The GPS signal cannot be received indoors.

    d. Plotting for individual location cannot be considered accurate without verification through alternative means.

    e. Calculations for speed or other data associated with movement of an individual GPS receiver cannot be made reliably.

By Authority Of:

Michael L. Brown
Chief of Police