Anchorage Police Department Regulations and Procedures Manual	Operational Procedures 3.10.065	
Policy and Procedure Title Mobile Data Computers	Effective Date 11/22/18	Page 1of 5
Replaces Prior Policy: 11/9/18	Approved by: Chief Justin Doll	

This Policy is for Departmental use only and does not apply in any criminal or civil proceeding. This Policy should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this Policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.

3.10.065 Mobile Data Computers

PURPOSE

The purpose of this General Order is to establish procedures and guidelines for the utilization of Mobile Data Equipment provided to Anchorage Police Department employees.

POLICY

It is the policy of the Anchorage Police Department to provide Mobile Data Computers ("MDCs") in order to enhance communication and the service provided to the community. The use of mobile computers reduces radio airtime, maximizes available information, provides access to DMV and criminal databases, and provides for the reporting of crimes and other incidents in a timely manner.

PROCEDURES

I. USE OF MDCs and SOFTWARE

A. Use of the MDC must comply with FCC rules and regulations as well as federal and state laws governing discrimination and sexual harassment. Employees using the MDC system (software & hardware) shall be personally responsible for the proper use of this equipment. All messages and information transmitted and viewed using the MDC must be duty-related and appropriate. Under no circumstances shall an employee using the MDC system broadcast anything that is in violation of Anchorage Police Department policies (e.g. Language and Prejudice 1.02.015C and Harassment 1.02.015O). This includes, but is not limited to, comments relating to sex, race, religion or any language that creates an intimidating, hostile or offensive work environment. Employees are reminded that the guidelines prescribed in the Radio Communications portion of the Regulations and Procedures Manual, specifically section 03.08.005, remain in effect and pertain to MDC usage. Employees are advised that electronic messages should be considered public domain and, as such, are subject to public records requests and civil and criminal law discovery requests. Electronic

messages and other information are stored, periodically reviewed by authorized Commanders, and subject to use in both criminal and civil matters.

1. VEHICLE-TO-VEHICLE MESSAGING SYTEM: Department personnel are restricted to duty-related use of the MDC Vehicle-To-Vehicle Messaging System. **MESSAGES OF A PERSONAL NATURE OF ANY KIND ARE PROHIBITED.**

2. The ability to operate the MDC while the vehicle is in motion does not relieve the driver of the duty to drive with due regard for safety, nor does it protect the driver from the consequences of operating the MDC while the vehicle is in motion if the operation of the MDC disregards the safety of others. See MDC Screensafe Program policy 3.10.085 for additional details.

3. Only Department personnel, who are specifically trained in its proper operation, including certification in installed software and databases, are authorized to sign onto and operate a mobile data computer.

B. The goal of this policy is to reduce non-priority voice traffic on the main APD radio frequencies. As a general rule, all voice traffic will receive a voice reply and all data traffic via the laptop will receive a data reply. Officers and dispatchers alike have the discretion to voice any transmission at any time. During times of system slow down or malfunction, operations will revert to all voice. Notification of such will be made over the main radio channel.

C. Employees are discouraged from being logged into CAD just for observation and monitoring purposes. The exception to this will be for those who are actively utilizing the MDC for research, system training, and/or testing. This section shall be adhered to in an attempt to have only those employees available for dispatches to be seen on the dispatch screen.

D. When off-duty, but still actively in their vehicle and mobile, officers will need to be logged into Inform Mobile on their MDC in the event they need to go out on the radio or self-assign to a call. The officer must select “TAC” in the sector section of the login screen. This would also be applicable to on-duty users who are not in their vehicle and not available to be dispatched (e.g., light duty assignment, research, training, and/or testing).

II. OPERATIONAL PROCEDURE

A. A voiced response from the officer requires no laptop input on his/her part except when logging on-duty at beginning of shift. The dispatcher will type all other voiced CAD transactions

B. The following radio traffic will be voiced by Dispatch:

1. All Code 3 or Code 4 calls;

2. All in-progress calls;

3. Updates to a call previously dispatched when a unit is not on scene (10-7). If pertinent comments are added to a call, especially officer safety

information or information that would change the priority of a call, Dispatch will verbally confirm the officer has received the updated information;

4. All locates that are of an urgent nature or that compromise officer safety. For all other locates, a CAD message will be sent to mobile units with a brief content description in the following format: **MSG MDC**, **broadcast** (the information from the locate);

5. All two unit calls unless there is significant information to lead the Dispatcher or Officer to believe the suspect has a radio scanner;

6. All calls of an urgent nature being held;

7. All cancellations on a call that has been dispatched;

8. All information that needs to be passed to an officer who is away from their laptop;

9. Dispatch has the discretion to voice any transmission at any time it is thought to be pertinent; and

C. The dispatcher will also advise by radio that a call is being sent on the MDC by use of the code "10-25" (old APD code meaning "respond to the area"). **Example***:* "22B1, 10-25…" The officer will acknowledge this voiced transmission.

D. The following radio traffic will be voiced by officers:

1. All traffic stops (10-70's);

2. All field interviews (10-76's);

3. All cover officer (10-34) requests;

4. All available for calls advisements (10-8's);

5. All traffic related to clear channels (10-44's);

6. Officers logging out on a unit they were not previously in route to;

7. All medic/fire requests;

8. Community Service Patrol, Impound, sand or roadway hazard requests will be verbalized on Channel 2 (to prevent multiple messages being sent by different officers for the same item);

9. An officer coming on duty;

10. Officers acknowledging they are in route as a cover officer (10-34);

11. Officers in route to or at lunch (10-80);

12. Whenever there is a "hit alert" on warrants from the laptop, the officer will voice to the dispatcher when a cover officer (10-34) is **not** needed. (The exception to this will be when the officer has already advised dispatch of the person being in custody (10-17) prior to running the "hit" on the laptop);

13. Officers have the discretion to voice any transmission at any time it is thought to be pertinent; and

14. Officers also have the discretion to not voice a transmission if needed to maintain operational security.

III. EQUIPMENT SECURITY

Safeguarding of the MDC is the user's responsibility. Due the expense of the equipment and the sensitive nature of the information available through the MDC, the following procedures will be followed.

A. All unattended vehicles with an MDC shall be:

1. Locked;
2. With the MDC locked in the docking station;
3. And the key removed from the docking station itself.

B. Any lost or damaged MDC equipment shall immediately be reported to a supervisor.

C. No one will attempt to install, delete, or modify any software or hardware associated with the MDC from the internet or other external sources without authorization from IT.

D. User passwords shall be kept confidential and not shared with other employees or the public.

E. Confidentiality

1. Access to APSIN, NCIC, and other databases are for official use only and inquiries of a personal nature are prohibited. Officers are encouraged to use the MDC as the primary source for all inquiries.
2. Release of confidential information to the general public is strictly prohibited. Information will include, but is no limited to:
    a) Criminal history information
    b) Intelligence files
    c) Department software, files, and databases
3. All officers will take into account their surroundings to prevent any unauthorized view to mobile computer screens containing confidential information or unauthorized access to the MDC by the public or non-sworn personnel.

IV. CARE AND MAINTENANCE OF EQUIPMENT

A. Daily Operation

1. Officers will exercise reasonable care in the use of mobile computers to minimize excessive wear or damage. Damage that is caused by carelessness or negligent actions of the employee may result in discipline.

2. Officers should inspect their MDC on a regular basis to ensure it is in working order. Any identified damage, inoperative or expired feature/software shall be reported in a timely manner to the Information Technologies Unit who is responsible for the administration and operational readiness of all Mobile Data Computers.
3. Report any lost MDC or disabling damage to a supervisor immediately.
4. Officers may need to warm up or cool down the interior of a vehicle prior to powering on depending on the vehicle's interior temperature.
5. Mobile computers must not be left in the vehicle during extreme cold or hot external temperatures.

V. ELECTRONIC CITATION PROCEDURES

Officer issuing electronic citations via the MDC under the authority of the Anchorage Police Department shall adhere to the following practices:

1. Officers shall use their Municipality of Anchorage-issued Department Serial Number (DSN) as their Unique Person Identifier.
2. Once authorized to issue electronic citations, officers must sign the Officer's Acknowledgement and Certification Form prior to issuing their initial electronic citation.
3. When issuing citations, officers must first log in using their own user name and password issued by the MOA. Upon completing and validating all information on the citation, the *Officer's Signature* line will display their printed name and DSN as an electronic signature. **Note:** An officer's electronic signature is the legally-binding equivalent of signing a citation by hand. Officers cannot deny responsibility for an electronically-issued citation bearing their printed name and DSN.
4. Officers shall at no time use a password or user name of another officer or allow another officer to use their password or user name to sign in to the system.
5. Should the need arise for officers to share a computer in order to issue a citation, each officer must sign in individually using their own unique user name and password.
6. Once a citation has been issued to a violator, officers shall not modify an electronic citation for any reason, except for adding information to the "Officer's Notes" field.
7. If a citation is issued in error or if a discrepancy is noted on the citation, the Officer shall be responsible for voiding the citation and notifying the Records unit.

*****END OF DOCUMENT*****