

AURORA POLICE DEPARTMENT

DIRECTIVES MANUAL

17.2	EFFECTIVE: September 1, 1998	Daniel J. Oates, Chief of Police
	REVISED: April 21, 2013	
SUBJECT: USE OF CAD AND MDC		
REFERENCES: COA: Information Security Policy, CCIS/NCIC and MDT Regulations		
		PAGE: 1 of 7

17.2 USE OF CAD AND MDC

This Directive, City of Aurora Information Security Policy and CCIC/NCIC Regulations govern the use of the CAD and MDC.

Any information available through the CCIC/NCIC terminal or MDC is limited to criminal justice purposes only. The criminal justice information system will not be queried for personal reasons, including but not limited to curiosity or other non-criminal justice investigation.

For the purposes of this directive, the MDC is considered an extension of the Aurora Police Department's law enforcement facilities.

17.2.1 Authorized Use of CAD and MDC

The CAD and MDC may be used to receive and send calls for service. The officer receiving the call will communicate when en route and at the scene by use of the appropriate function buttons. Officers operating the MDC while their vehicle is in motion, are not relieved of responsibility if an accident occurs.

The CAD and MDC may be used to send and receive official messages from one terminal to another. "Be-on-the-look-out" and official messages may be sent to all terminals.

Non-criminal reports may be made on the CAD and MDC systems.

The MRE module of the MDC will be utilized for completing and submitting official police reports. Dispositions or remarks will be added to criminal cases on the CAD and MDC. This will not replace an offense report.

Some CCIC/NCIC functions may be done on the CAD and MDC systems. These functions include, but are not limited to want and warrant checks, driver license information, VIN, and vehicle license information.

Members may only access CCIC/NCIC through approved hardware located within an Aurora Police Department law enforcement facility. The portability of the MDC allows members access to criminal justice information systems from various

locations, in and around the jurisdictional boundaries of Aurora. Members may only access CCIC/NCIC for official business related to an actual investigation.

CAD and MDC may be used instead of the police radio when necessary for silent communication.

Members are authorized to remove the MDC from the vehicle for the purposes of completing necessary forms required for a specific investigation. Members remain responsible for the accountability of the MDC and will ensure that the MDC is returned to the assigned vehicle. When docking the MDC, members will exercise caution to ensure proper alignment to prevent damage to the mount or computer.

Command officers of specialty units will develop Standard Operating Procedures to govern the use of MDCs assigned to his/her operational element. The command officer of the unit is responsible for the accountability of all computers assigned to his/her unit.

Accessing the internet via the MDC is limited to the links provided on the Resource page or links provided for special assignments. These links are provided for members to access those sites needed for the users to use for official business. If a member discovers a link not on the resource page that would be beneficial to other members in the performance of their duties, the member will submit a request to the Electronic Support Section for that link to be added to the Resource page. The Electronic Support Section will discuss the need with the Information Technology Department (ITD). If the link is determined to be a benefit to the performance of official duties, it will be added to the Resource page. Members will not access the internet for personal use or benefit.

17.2.2 Unauthorized Use of CAD and MDC Systems

The CAD and MDC will not be used for unauthorized personal messages or unnecessary comments or opinions.

No obscene or profane language may be used on the CAD or MDC Systems. Because of CCIC/NCIC regulations, criminal histories may not be run from the MDC's. Only members certified and authorized through CBI may run Criminal histories. Criminal histories will only be conducted for official police business in conjunction with an actual investigation.

Members are not permitted to utilize an MDC outside the defined work environment (e.g., taking a MDC home to access CCIC/NCIC) without specific authorization. Command officers may approve the use only when the assignment is directly related to an ongoing investigation and overtime has been authorized. An exception to this directive exists when equipment/applications require evaluation. All testing of equipment will be conducted at the direction of the Electronic Support Section.

17.2.3 MDC Reports / Remarks

Following is a list of information a member may include when adding remarks to a call or completing an MDC report.

- a. Last name of reporting officer.
- b. Name(s) of person(s) involved (unless the individual is a juvenile).
- c. Date of birth of person(s) involved (unless the individual is a juvenile).
- d. Summons number.
- e. Estimated amount of property damage or loss.
- f. A brief account of the incident and action taken.
- g. Names of juveniles, however, these must be redacted before release to the public.

The following information will not be entered when adding remarks or completing an MDC report.

- a. Names of Child Abuse/Neglect suspects, victims or reporting parties.
- b. Names of Sexual Assault victims.

17.2.4 Incident Numbers and Report Numbers

Each incident and service assignment is assigned a number, automatically, by the Computer Aided Dispatch (CAD) system. When the incident is criminal in nature, requires a written report, or results in the issuance of a criminal or criminal traffic summons, the officer will request a report number be assigned to the incident. Officers may request a report number through functions in the MDC or by asking a dispatcher.

Incident / Report numbers are issued in a chronological order and are not repeated.

17.2.5 Security of Terminals

CCIC By-Laws require 24-hour supervision for terminals at any location. Terminals not meeting this requirement will be closed at the end of the working day. Members operating department vehicles equipped with an MDC will be cognizant of the information displayed on the screen. Members will take precautions to prevent the unauthorized viewing of regulated and/or confidential information by arrestees, passengers to include “ride-a-longs” and any other citizen. When out of the vehicle, at a minimum, members will ensure that all vehicle doors are locked and the display screen is either closed or sent to black (FN-F3).

At the end of a shift, members will ensure that assigned MDCs are completely logged off and powered down. The member will verify that the MDC is securely locked in the dock. All doors to the vehicle will be locked. If for any reason the vehicle cannot be secured, the MDC will be stored and logged in the Patrol Lieutenant's file cabinet.

MDCs will not be stored in vehicles without a locking docking station installed into the vehicle.

Because of licensing agreements and access restrictions, computers logged into Versadex with no activity for two hours will automatically be disconnected. Members are encouraged to disconnect from Versadex when not actively working in the system.

All members of the department share in the responsibility of ensuring the integrity and confidentiality of all criminal justice information.

"CBI reserves the right to immediately suspend furnishing criminal history data to the user when either the security or dissemination requirements approved by the NCIC Advisory Policy Board and adopted by the NCIC and/or CBI is violated."

It is the responsibility of all members of the Aurora Police Department to ensure the "integrity and effectiveness" of criminal justice information. The Chief of Police has agreed that exchange of computerized criminal history information will be according to CCIC By-Laws.

17.2.6 Passwords and Systems Security

Members are prohibited from signing on or logging into CAD or MDC, by using an OSN, I.D. number, or password other than their own. A member finding that their own OSN, I.D. number, or password will not allow them to log in will report that fact immediately to the Records Unit or IT Help Desk.

17.2.7 MDC Installations

The MDC's will be installed in patrol and specialty vehicles. The placement of additional MDC's will be based on the needs of the Department. Every vehicle equipped with a MDC will be issued a key to the MDC dock. This key will be kept on the vehicle key ring and will not be removed.

The Information Technology Department (ITD) will install inventory tags on all MDC's. These tags include the bar code label and vehicle assignment. These identification labels will only be placed onto MDC's by members of the ITD. Removal of these tags/labels is strictly prohibited by any other member of the department.

In addition, the MDC system requires periodic updates. Many of these updates will occur via the City Wi-Fi network. On occasion, the complexity of the upgrade requires physical, hands-on programming of each computer. In these situations, the Electronic Support Section will mark completed vehicles with tags on the rear window of the vehicle. It is essential that these tags remain in place until the entire process is complete. The Electronic Support Section will notify members when removal of the tags is authorized.

17.2.8 Inspections

Prior to signing on a MDC, the member will examine the hardware for damage and/or missing parts. The member will check the Vehicle Inspection Log book to determine if the damage or missing equipment was previously reported. Any observed damage or missing parts not noted in the Vehicle Inspection Log book will be immediately reported to the member's supervisor. The supervisor will note the reported damage or missing equipment in the Vehicle Inspection Log Book. Members will confirm the correct MDC is in the vehicle they are assigned (MDC will have the car number on the lid). If the MDC in the vehicle is not assigned to that vehicle, the member will immediately notify their supervisor. The supervisor will immediately notify a Electronic Support Section supervisor via e-mail and notify ITD via the MDC help line (extension 3-MDCP).

17.2.9 Damage and Reporting of Damage

Members noting a malfunction or damage to a MDC will contact their immediate supervisor. The supervisor will inspect the MDC and determine the functionality of the equipment. The supervisor will complete a vehicle repair request form. If the damage does not affect the functionality of the MDC, the supervisor will note the damage in the vehicle logbook and submit the repair request to the ITD Radio Shops. The MDC will be left in-service.

If the damage affects the functionality of the MDC, the vehicle should be deadlined. The repair request will be given to the district courier for transport of the vehicle with MDC mounted to the radio shops for repair. The MDC will be left in the vehicle's docking station.

If the supervisor determines the damage was caused by a malicious or negligent act, the supervisor will notify the chain of command and the Electronic Support Section Lieutenant and initiate the initial inquiry.

If the MDC comes into contact with liquid, immediately power down the MDC and undock the hardware. The MDC should be tilted in such a manner to allow any liquid to escape from the unit. The member will immediately notify his/her supervisor. The supervisor will notify a Electronic Support Section supervisor via e-mail and cause the MDC to be taken to the Radio Shops. Do not restore power to the MDC as electrical shock and irrevocable damage may occur.

17.2.10 Cleanliness

Members will use only the approved screen cloth to clean the MDC screen. The use of any cleaning liquids will cause permanent damage to the screen. Members will use only their finger or department issued stylus to manipulate the MDC touch screen.

17.2.11 Unauthorized Installation of Software and Reconfiguration of MDC's

Because of the sensitive nature of the multiple software applications required to efficiently run the MDC system, members will not reconfigure the MDC in any manner, to include (but not limited to):

- Changing the appearance of the background
- Changing the method in which the programs launch
- Changing the appearance of the cursor
- Download or install any software or programs not approved by the Electronic Support Section and /or ITD
- Changing the manner the MDC operates in any way not approved by the Electronic Support Section and/or ITD.
- Will not remove the screen protector from the MDC.

Members will immediately notify their supervisor if any of the above changes are observed to an MDC they are assigned. Members are allowed to accept official Department upgrades via the City Wi-fi system.

Members of the Electronic Support Section and ITD are allowed to load approved items to the MDC's. The Public Safety Systems Manager is the final approving authority.

17.2.12 Security of MDC's

When a vehicle equipped with a MDC is left at the city shops, for repairs or service, the MDC can be left inside the locked and secured vehicle. The MDC must be locked into the docking station. The MDC must be removed from the vehicle if left over night at any location other than the city shops for repairs or service.

Members will be responsible for ensuring the MDC's from vehicles left over night at a repair facility are turned in to the Radio Shop. MDC's removed from vehicles will only be stored at the Radio Shop. Watch Commanders will ensure that MDC's taken from vehicles outside of the regular business hours of the Radio Shop are secured at the District Stations; and as soon as is feasible the MDC will be taken to the Radio Shop for long term storage.

When an MDC is in need of repair or fails to maintain connectivity, the MDC and the assigned vehicle should be transported to the city radio shops (with the MDC installed) during normal business hours.

17.2.13 Docking and Undocking of MDC's

Members may undock and utilize the MDC in a portable fashion for investigative purposes. The security of the MDC remains the responsibility of the assigned member.

When returning the MDC to its assigned vehicle, special care must be exercised to insure the sliding docking panel door is open and the MDC is properly aligned in the dock.

MDC's will only be installed into specifically assigned vehicles. Changing equipment, software and accountability dictates the need for MDC's to be assigned to specific vehicles. Additionally, as the Department has different model MDC's and corresponding mounts, switching an MDC from the assigned vehicle to another vehicle may cause damage to the MDC or the mount or may create problems with connecting to the network.

17.2.14 Air Cards

Air cards are assigned to a specific MDC and will not be removed and or switched with other air cards except by members of ITD or the Electronic Support Section. Members noting damaged to or missing air cards will immediately notify their supervisor.

17.2.15 Global Positioning System (GPS)

Members will not block, interrupt or otherwise disrupt the GPS installed in vehicles or MDC's.

GPS data on police vehicles will be retained for one year and then destroyed unless specifically requested by an appropriate authority in connection with litigation, a criminal investigation or an internal investigation.