

Mobile Data Center Use

421.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper access, use, and application of the Mobile Data Center (MDC) system in order to ensure appropriate access to confidential records from local, state, and national law enforcement databases, and to ensure effective electronic communications between department members and the Communications Center. See the CJIS Access, Maintenance, and Security Policy for additional guidance.

421.2 POLICY

Louisville Police Department members using the MDC shall comply with all appropriate federal and state rules and regulations and shall use the MDC in a professional manner, in accordance with this policy.

421.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to messages accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use Policy for additional guidance).

421.4 RESTRICTED ACCESS AND USE

MDC use is subject to the Information Technology Use, Protected Information, and CJIS Access, Maintenance, and Security policies.

Members shall not access the MDC system if they have not received prior authorization and the required training. Members shall immediately report unauthorized access or use of the MDC by another member to their supervisors or Shift Supervisors.

Use of the MDC system to access law enforcement databases or transmit messages is restricted to official activities, business-related tasks, or communications that are directly related to the business, administration, or practices of the Department. In the event that a member has questions about sending a particular message or accessing a particular database, the member should seek prior approval from their supervisor.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing, or any other inappropriate messages on the MDC system is prohibited and may result in discipline.

It is a violation of this policy to transmit a message or access a law enforcement database under another member's name or to use the password of another member to log in to the MDC system unless directed to do so by a supervisor. Members are required to log off the MDC or secure the MDC when it is unattended. This added security measure will minimize the potential for unauthorized access or misuse.

421.4.1 USE WHILE DRIVING

Mobile Data Center Use

Use of the MDC by the vehicle operator should be limited to times when the officer is operating the vehicle at less than 20 mph and/or the vehicle is stopped. The Louisville Police Department utilizes the Archangel System, which is technology to disable the track pad and touch screen of an officer's MDT when the vehicle reaches a pre-determined speed of 20 mph. However, the screen remains visible and active up to 79 mph. At 80 mph, the screen will lock and the operating system will not be visible. The computer will re-engage when the officer stops or the vehicle speed is less than 20 mph. Information that is required for immediate enforcement, investigative, tactical or safety needs should be transmitted over the radio (CRS § 42-4-201).

In no case shall an operator attempt to send or review lengthy messages while the vehicle is in motion.

At no time when the vehicle is in motion should the display be viewed by the driver for visual entertainment, including Internet browsing or the use of social media or email.

421.5 DOCUMENTATION OF ACTIVITY

Except as otherwise directed by the Shift Supervisor or other department-established protocol, all calls for service assigned by a dispatcher should be communicated by voice over the police radio and electronically via the MDC unless security or confidentiality prevents such broadcasting.

MDC and voice transmissions are used to document the member's daily activity. To ensure accuracy:

- a. All contacts or activity shall be documented at the time of the contact.
- b. Whenever the activity or contact is initiated by voice, it should be documented by a dispatcher.
- c. Whenever the activity or contact is not initiated by voice, the member shall document it via the MDC.

421.5.1 STATUS CHANGES

All changes in status (e.g., arrival at scene, meal periods, in service) will be transmitted over the police radio or through the MDC system.

Members responding to in-progress calls should advise changes in status over the radio to assist other members responding to the same incident. Other changes in status can be made on the MDC when the vehicle is not in motion.

421.5.2 EMERGENCY ACTIVATION

If there is an emergency activation and the member does not respond to a request for confirmation of the need for emergency assistance or confirms the need, available resources will be sent to assist in locating the member. If the location is known, the nearest available officer should respond in accordance with the Officer Response to Calls Policy.

Members should ensure a field supervisor and the Shift Supervisor are notified of the incident without delay.

Mobile Data Center Use

Officers not responding to the emergency shall refrain from transmitting on the police radio until a no-further-assistance broadcast is made or if they are also handling an emergency.

421.6 EQUIPMENT CONSIDERATIONS

421.6.1 MALFUNCTIONING MDC

Absent supervisor approval, members will not use vehicles with malfunctioning MDCs. Whenever members must drive a vehicle in which the MDC is not working, they shall notify the Communications Center. It shall be the responsibility of the dispatcher to document all information that will then be transmitted verbally over the police radio.

421.6.2 BOMB CALLS

When investigating reports of possible bombs, members should not communicate on their MDCs when in the evacuation area of a suspected explosive device. Radio frequency emitted by the MDC could cause some devices to detonate.

