	BRIDGEPORT POLICE DEPARTMENT POLICY AND PROCEDURE GENERAL ORDER	Distribution ALL PERSONNEL	General Order Number **5.12**
		Original Issue Date 5/21/19	Reissue/Effective Date 10/11/19
Order Title: **MOBILE DATA TERMINALS**		Accreditation Standard: POSTC: 2.5.19	Section 5
		Section Title PATROL FUNCTIONS	
Rescinds: N/A		**Armando J. Perez, Chief of Police**	

This General Order is for departmental use only and does not apply in any criminal or civil proceeding. This General Order 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 General Order 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

I. PURPOSE:

The purpose of this General Order is to establish procedures and guidelines for the utilization of Mobile Data Equipment provided in Bridgeport Police Department patrol vehicles.

II. POLICY:

It is the policy of the Bridgeport Police Department to provide Department Mobile Data Computers ("mobile computers") in order to enhance radio communications and to provide sworn employees with a measure of safety through information awareness and aid in accomplishing community service. The use of mobile computers also reduces radio airtime, maximizes available information, provides access to criminal databases and DMV, and provides for the reporting of crimes and other incidents in a timely manner.

III. DEFINITIONS

Information Technologies: Members of the City of Bridgeport's Information Technologies Department and Bridgeport Police Department members who are assigned to oversee and maintain the Department's computers and electronic communications equipment.

IV. PROCEDURES:

A. Management of Mobile Computers

1. The Department's Information Technologies Unit is responsible for the administration and operational readiness of all Mobile Data Computers and will provide Mobile Data Computer training to all officers.
2. Employees will inspect each mobile computer and console during vehicle

inspections for signs of damage or disrepair.

3. Designated staff may enter, review, and monitor information stored on mobile computers at any time without advance notice. Periodic inspection of mobile computer traffic logs will take place at the direction of the Chief of Police.

B. Use of MDTs and Software

1. All traffic transmitted using the mobile computer must be business-related and comply with the same quality standards as voice traffic. The mobile computer will not be used for personal or recreational purposes, and messages shall not contain derogatory references to other personnel or agencies, or contain any text a reasonable person would find offensive. Downloading or transmitting materials that contain obscene or disparaging language or graphics is strictly prohibited.

Employees are hereby advised that there is NO EXPECTATION OF PRIVACY concerning the sending or receiving of messages on the Department's Mobile Data Computer System.

2. Only Department personnel, who are specifically trained in its proper operation, including certification for mobile COLLECT/NCIC operation, are authorized to sign onto and operate a mobile computer. Under no circumstances will individuals from outside the Bridgeport Police Department be permitted use of Department mobile computers without prior authorization from the Chief of Police, or designee.
3. User passwords shall be kept confidential and not shared with other employees or the public.
4. In the interest of officer and citizen safety, officers should not attempt to read the mobile computer screen or interact with the touch screen or keyboard while the vehicle is in motion. An exception to this procedure may occur when the cruiser is a two-officer unit, and the officer seated in the front passenger's seat is operating the computer.
5. Officers will be able to adjust Department mobile computers and their mounting systems so that they are at a comfortable working position. The mobile computer's adjustable position will allow officers access to the cruiser's radio microphone and dashboard controls.
6. While the cruiser is being operated, Department mobile computers will not be placed in such a position so as to affect the deployment of the passenger side airbag.
7. Information Technologies will be charged with the responsibility of installing all software applications onto Department mobile computers.
8. No one will attempt to install, delete, or modify any software or hardware

associated with a mobile computer without authorization from the Information Technologies. Personal software is not to be downloaded or installed on any mobile computer without prior written authorization from the Information Technologies. Any unauthorized software may be cleaned from the device at random, and the Department will not be liable for its loss.

9. In no case will external materials or applications be downloaded onto mobile computers. To prevent viruses, no material shall be downloaded or installed from the Internet or other external sources. Employees may be held accountable for any damage cause by unauthorized software to the mobile computer.

C. Restrictions

1. Officers are prohibited from accessing sites or engaging in e-mail pertaining to sexual content, hate groups, chat rooms, merchandising, etc., unless instructed to do so in conjunction with a special assignment or investigation.

Any message containing slang or language that could be construed as a slur or sexual harassment against any person or group is not authorized nor permitted.

D. Confidentiality

1. Access to COLLECT/NCIC is provided for official use only and inquiries of a personal nature are prohibited. Officers are encouraged to use the Mobile Data Computer as the primary source for all inquiries. Radio inquiries should be reserved for urgent requests while the vehicle is in motion to ensure officer safety or in situations when it is not feasible to do so.
2. Any information sent or received on a mobile computer is confidential and will only be disseminated as directed by COLLECT/NCIC regulations and any other applications under the Connecticut Criminal Justice Information System (CJIS) umbrella. Release of confidential information to the general public that is accessible from the mobile computer is strictly prohibited. The general public includes family members, friends and ride-alongs that are not law enforcement employees.
3. Confidential information will include but is not limited to:
    a. Criminal history information
    b. Intelligence files
    c. Department software, files, and databases
4. 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 mobile computer by the public or any non-sworn personnel. Mobile computers will not be left unattended in public places or residences at any time except in cases of extreme emergency.

A supervisor will be immediately notified of any breach in confidentiality.

E. Operating Procedures

1. Officers can receive call-for-service information on their mobile computers, and then acknowledge receipt. Car-to-car messaging is encouraged to reduce radio traffic. Messages are generally considered public information. Officers may also acknowledge receipt of information over the radio, and dispatch will perform the function and/or updates through the Computer Aided Dispatch (CAD) system.
2. Logging on the mobile computer:
    a. Officers will turn on the power for Department mobile computers.
    b. Once Department mobile computers have been powered on, officers will be presented with a logon screen.
    c. To access Department mobile computers, officers will be required to logon with a user ID and password.
    d. When cruisers are shut off, Department mobile computers continue to run off the cruiser's battery for a designated period of time. When the designated time has been achieved, the mobile computer will shut down. Note: If a shutdown should occur, officers will have to log back into the mobile computer upon his/her return. Officers will not be required to turn off Department mobile computers when leaving their cruiser for a short period of time.
3. Logging off the mobile computer
    a. At the end of the officer's shift, he/she will log off the mobile computer and power off the computer.
    b. To power off the mobile computer, officers must first log off and EXIT the system application.
    c. From the Shutdown dialogue window, officers need to select the shutdown option for the mobile computer.
    d. The sequence will properly shutdown and also power off the mobile computer.
4. Officers who experience technical difficulty with the mobile computer will immediately contact the Supervisor or IT Personnel, if on-duty.

F. Security, Care, and Maintenance of Equipment

1. Officers will exercise reasonable care in the use of mobile computers to minimize excessive wear or damage. Sharp objects shall not be used to access the touch screen. Damage that is caused due to normal use will be covered under warranty agreements with the manufacturer. Damage that is caused by carelessness or negligent actions of the employee may result in discipline.
2. At the beginning of each shift, the officer will inspect the mobile computer for

any signs of damage or disrepair and immediately report any findings to his/her Supervisor. Officers will perform the log on procedure for CAD and COLLECT/NCIC. At the conclusion of each shift, the officer will properly shut down the mobile computer.

3. Officers will keep the mobile computer screen and keyboard clean using the supplies provided. Paper products are not to be used to clean the screen. Food and liquids must be kept away from the mobile computer at all times. In the event of an accidental spillage, the officer will:
    a. Log off of all active sessions and shut down the mobile computer as quickly as possible
    b. Clean the affected area as trained
    c. Make arrangements, through his/her supervisor, for the Information Technology Unit to inspect the mobile computer.
4. An officer's vehicle will not be jump-started, or used to jump-start another vehicle, with the Mobile Data Computer installed.
5. When away from the vehicle, officers must ensure that the vehicle is locked to prevent unauthorized use of the mobile computer.
6. Mobile computers will not be used as a workbench, clipboard holder, shelf, cup holder etc. Note: paperclips should not be placed on Department mobile computers as they may fall inside corrupting its hardware, which could result in a failure of the system.
7. The interior environment of the cruiser must be within a temperature range of 40-95 degrees Fahrenheit in order to power on Department mobile computers. Officers may need to warm up or cool down the interior of a vehicle prior to powering on, depending on the cruiser's interior temperature. During hot weather, officers should lower rear windows one-half inch to allow air circulation for the cruiser's interior, which can aid in preventing overheating.
8. Mobile computers needing to be repaired will only be removed at the direction of the Department's Information Technologies Personnel or a Department designated repair vendor.
9. If officers experience any problem with a mobile computer, they will fill out a vehicle maintenance request form. The form will be submitted to the officer's supervisor. The supervisor will review the form and forward the form to the Information Technologies Unit.
10. Suggestions on improvements to Department mobile computers will be directed to the officer's immediate supervisor, who will forward them through the chain of command.