# Stowe Police Department

| | |
|---|---|
| **General Order:** 1.30<br><br>**VT CJIS Mobile Data** | **Related General Orders:**<br>1.19 Mobile Communication Device<br>1.22 Mobile Data Computers |
| This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline. | |
| **Applicable Vermont Statutes:** | |
| Issued By: Donald B. Hull, Chief of Police | |
| Date Implemented: 06/18/2012 | Date Revised: 04/14/2015, 07/30/2018 |

## I. PURPOSE:

1. To provide guidelines and procedures for the use of Mobile Data Computers (MDC). Mobile Data Computers are used for communication between NLETS/VLETS, Vermont Department of Motor Vehicles records, VIBRS and Mobile Data Computer equipped police cruisers as well as those computers utilizing Valcour.

2. The Stowe Police Department Mobile Data Computer system utilizes software that allows members in the field direct access to NLETS, VLETS and NCIC information through the use of Valcour on MDC. Members will also have access to Valcour program, the departmental e-mail system, as well as several other applications deemed appropriate to meeting the needs of the department.

## II. DEFINITIONS:

**Vermont Wireless Information Network (VWIN):** VWIN is a wireless mobile data network for interested state and local Vermont government agencies which provides access to:

VIBRS (Vermont Incident Based Reporting System);
NCIC (National Crime Information Center);
NLETS (National Law Enforcement Telecommunications System).
SPIN (State Police Information Network)

A. VWIN uses mobile data computers to send and receive encrypted and compressed data.

B. VWIN is managed and supported by the Vermont Department of Public Safety.

**Mobile Data Computer (MDC):** A lap-top, tablet (IPAD) or other version of a personal computer

## III. PROCEDURE:

***SECURITY***

1. The security of the system will be the concern of all users. All NLETS/VLETS/NCIC/VIBRS/SPIN rules and regulations regarding use and disclosure of information are in full effect when operating Mobile Data Computers. The computers have been designed with both a Windows log on and password prompt as well as a log-on identification/password system (Secure Remote). The Secure Remote password system will be managed by Criminal Justice Services. The VWIN/Aircard system will use a minimum of 128 bit encryption as required by CJIS Security policy.

2. The person to whom the MDC is assigned is responsible for insuring the security of the computer against unauthorized use.

3 MDC's will be placed in a docking station or mounting bracket in the vehicle if available.

4. All information obtained via the MDC computers will be treated as CONFIDENTIAL and used for authorized law enforcement or criminal justice purposes only.

6. If it is believed unauthorized access was attempted or occurred or if it is believed that a security breach has occurred i.e. sensitive or confidential data has been compromised or if the computer has been lost or stolen the person to which the computer is assigned shall immediately contact and advise his/her supervisor. The Officer shall also comply with all other Stowe Police Rules and Regulations regarding the loss of or damage to equipment.

7. No confidential material will be stored on the mobile computers. All personnel will ensure that prior to the end of their shift that the all files saved in the appropriate programs. Any e-mail or instant message that contains sensitive or confidential data received during the shift must be deleted and or destroyed. Any paper copy of any e-mail, instant message or message received from VLETS/NLETS will be shredded as per the NCIC policy.

8. Anti-virus is in place on all MDC's. Updates to the anti-virus protection are downloaded to the MDC automatically.

***WARRANTS/STOLEN PROPERTY***

1. Information indicating a warrant/stolen property from NCIC may constitute probable cause. However, arrest warrants **must** be confirmed with the originator of the information to determine that the warrant(s) are still active and accurate. Members must determine, to the best of their ability, the subject/object is the same as the warrant/stolen property in NCIC. All District Court warrants are considered accurate and valid.

2. When members receive notification of a "VCIC/NCIC" hit, they shall immediately contact either their local PSAP via cruiser radio. The member shall request confirmation of the warrant/stolen property by the PSAP tele-communicator **prior to taking a subject / object into custody**. The same procedure will be followed prior to acting on any other "hit" from the VCIC/NCIC system. The possible hits may include but are not limited to Temporary / Final Relief from Abuse Orders, Sexual Offender information and FBI terrorist alerts.

***RECORDS MANAGEMENT SYSTEM***

1. Members are encouraged to utilize the MDC to enter information into the records management system (Valcour) software residing on each MDC.

***MESSAGING***

1. MDC messaging is defined as any message sent or received from one MDC to another

2. MDC messaging, on a department MDC, shall be used for department business and is subject to the following restrictions:

A. The message shall have a reasonable communicative purpose.

B. Messages must be authored in a professional business-like manner, which would be considered acceptable as public record.

C. The communication shall not be used to harass, annoy or alarm any recipient or third party.

D. The communication shall not contain language, acronyms or symbols representing language that would be considered offensive or obscene to a reasonable member of the public.

E. The content shall not bring discredit to any public safety employee (including coworkers) or public safety agency.

F. The content shall not bring unwarranted discredit to a member of the public.

G. The communication shall not contain any home address or telephone number of law enforcement personnel unless that employee has given express permission to transmit the information.

H. The communication shall not contain any slanderous statements toward any group, organization or individual.

J. Personnel should clearly understand that information viewed and obtained is similar to other VLETS/NCIC information and any information received via the MDC shall be kept confidential.

K. MDC messages and CAD calls may be public record. Any request for information that could be considered a public record should be referred to the Chief of Police. This does not preclude a field user from using information provided by the MDC to satisfy legitimate law enforcement purposes.

***MAINTENANCE / REPAIRS***

1. Members are required to notify a supervisor or the department technology officer of any problems with the MDC or when a MDC is not functioning properly. The MDC will be turned over to the assigned representative, who based on the problem presented, shall forward the MDC to the appropriate individual for service.

***GENERAL CARE & USE***

1. MDC's will be placed in a docking station or mounting bracket in the vehicle if provided

2. No software or material will be loaded into the MDC without prior approval.

3. Members shall not willfully damage or permit any MDC to be damaged.

4. Department personnel will adhere to any law that pertains to the operation of a vehicle while using an MDC. The operator of the police vehicle shall not type messages or entries while the vehicle is in motion.

5. MDC's may be assigned to specific vehicles or to specific individuals.

6. MDC's will not be left in a vehicle when the officer is off-duty or the vehicle is not being used.

7. Personnel that are logged on to the MDC shall ensure that their current and correct status is provided at all times. Personnel shall log off the MDC at the end of their shift and whenever the MDC will be left unattended for an extended period of time.

8. Personnel shall secure the vehicle (i.e., lock the doors and trunk) to prevent theft or unauthorized use of and/or tampering with an MDC.

## III. RAMIFICATIONS FOR NON-COMPLIANCE/ENFORCEMENT

1. Agencies and users of Mobile Data Computers shall adhere to this policy and any other mandatory rule, policy or procedure or could be sanctioned by the Stowe Police Department or the VIBRS staff of the Division of Criminal Justice Services as deemed appropriate by the VIBRS Advisory Board.

2. Sanctions could result in a loss of privileges (disconnection) by the user.

3. The Chief of Police or her/her designee may impose emergency sanctions, including disconnection, if he/she believes there is a security threat sufficient to warrant such action.

## IV. DISCIPLINE:

Any violation of this policy may be grounds for disciplinary action consistent with any applicable collective bargaining agreement, statute, Department policy or Town policy.