	POLICY & PROCEDURE	SERIES # **549**	PAGE 1 OF 6
	SUBJECT **MOBILE DATA TERMINALS**		EFFECTIVE DATE **07/12/05**
			OVERSIGHT **Operations**
	DISTRIBUTION **ALL MANUALS**	AMENDS/SUPERSEDES/CANCELS P&P # NEW POLICY: Cancels Section IX of P&P 534	

I. PURPOSE:

The purpose of this policy is to establish guidance in the installation, operation, maintenance and security of the Mobile Data Terminal computers owned by the Hampton Police Division. This policy sets forth the guidelines for access to, and dissemination of data contained in local, state, and national computer systems.

II. POLICY:

The Hampton Police Division maintains mobile data terminal computers to provide increased effectiveness and efficiency of work effort through access to other information systems (NCIC/VCIN) through communications interfaces. It is the policy of the Hampton Police Division to: 1) control the configuration of computer systems; 2) distribute software only in accordance with license agreements; 3) ensure security and privacy of data stored on computer systems operated by the Division, and 4) limit the use of police computer systems to official police business and other uses as permitted by the Chief of Police.

Furthermore, system use is governed by Division policies, City policies, and local, state and federal laws. Use of systems owned and operated by the Division will: 1) be ethical; 2) be constrained in the consumption of shared resources; 3) demonstrate respect for official information, ownership of data, and system security mechanisms; 4) be respectful of individuals' rights to privacy and their rights to freedom from intimidation and harassment.

The Special Projects Unit shall have overall responsibility of the MDT program, and the assignment of MDT units. The Division's Systems Analyst will serve as the Administrator of the system itself.

III. DEFINITIONS:

Mobile Data Terminal (MDT): A computer, placed in a vehicle, which is used through special programming, to send and receive data packets via radio transmission without the use of voice communications.

Computer Aided Dispatch (CAD): CAD is the system used by the Hampton Police Division to dispatch calls for service and handle complaints.

IV. PROCEDURE:

A. MDT CAPABILITIES:

1. NCIC/VCIN and DMV inquiries
2. PISTOL Records Information
3. Car-to-car messaging
4. CAD information retrieval
5. View calls for service

B. USES AND RESTRICTIONS:

1. The Mobile Data Terminals may be utilized for NCIC and VCIN checks, DMV records, and to obtain information from the internal PISTOL Records Management System. Calls for service that are “Low Priority” in nature will be assigned to the district officer for his/her response. Road Supervision will be responsible for the proper handling of these calls and see that they are handled within the time constraints defined in Policy & Procedure 1408. The responding officer or supervisor will address calls that result in time delay by contacting the complainant/victim.

   “Low Priority” calls in districts that are not MDT equipped will be the responsibility of Communications.

   All “High and Normal” priority calls and any call that necessitates the dispatch of more than one unit will be verbally dispatched and monitored by Communications personnel until the completion of the event.

   a. MDT’s are not to be utilized to communicate with dispatchers in lieu of radio communications. If a call for service is verbally dispatched, those officer(s) dispatched will verbally mark enroute, on-scene and clear those calls.

   b. Officers may issue themselves an IBR number for an Incident they are dispatched to. Officers will add notes to calls as needed. If the nature of the call changes, Officers are to change the “Nature Code” that was assigned to the call.

   c. Officers may clear a complaint they are dispatched to and utilize the prescribed MDT Disposition Codes available. If the disposition requires further explanation, Officers will use the Notes field.

   d. Only supervisors in the field are to converse with Communications personnel via the MDT using car-to-dispatch messaging. Officer to dispatch messaging will not be permitted.

2. Public Safety Communications has the sole responsibility for dispatching calls for service. If a “silent dispatch” call escalates to a higher level, Communications Personnel will intervene and dispatch the call. (See

Policy and Procedure #1408 “Dispatch Operations”)

3. Officers who are driving will only operate the MDT while their vehicle is stopped or parked. Operation of the MDT by a driver while their vehicle is in motion is strictly forbidden. Therefore, the following self-initiated calls for service will not be permitted by officers in the field: traffic stops, pursuits or the stopping of suspicious persons/vehicles. Such calls are considered Officer Safety calls and will be monitored by the dispatcher.

4. All MDT messages are recorded and subject to the Freedom of Information Act. Good judgment should always be exercised in preparing the context of all messages so as not to bring reproach or ridicule to you or any other person, or cause embarrassment to the Division.

5. Misuse of the MDT system will be considered grounds for disciplinary action, and possible criminal prosecution.

6. Information obtained from NCIC/VCIN, Division of Motor Vehicles (DMV), and Pistol databases is privileged information and is to be accessed for **law enforcement purposes only**.

C. TRAINING: All officers operating a MDT shall complete MDT Visual and VCIN Level “C” training during their departmental post academy class. The System Administrator will set up an account and approve all passwords for the MDT system.

D. INSPECTION: Upon entering a vehicle at the start of each shift, officers shall check the MDT to insure that it is operable, and has not been damaged. Any damages observed must be reported immediately to a supervisor. The officer will complete a Special Report detailing the damage, and contact the System Administrator for repairs.

E. CARE OF EQUIPMENT: Due caution must be exercised in the care and handling of the MDT. The placing of drinks, food, clipboards, or other objects upon its components can cause damage to the unit and is strictly prohibited.

F. MAINTENANCE:

1. Vehicle out of Service – When the vehicle is taken to the city garage, Atlantic Communications, or any other department-approved facility for repairs, the radio and modem should be powered off. If the vehicle is to be out of service for an extended period of time the Special Projects Office will be notified and determine if the MDT should be removed. If the MDT has been removed, the System Administrator will be notified when the vehicle is back in service to have the computer reinstalled in the vehicle.

2. Damage – Supervisors shall be responsible for inspecting the MDT in a vehicle involved in a vehicular accident for damages caused by the accident. If the vehicle and computer are operable, the computer will

remain in the vehicle until such time as the vehicle is ordered to the body shop for repairs.

3. Computer not working – If an individual computer is inoperative, the officer will notify his/her supervisor and make an appointment with the System Administrator by calling during normal business hours, or leaving a phone mail message on extension #6803. Reasonable efforts will be made by the System Administrator to examine the MDT in a timely manner.

4. System Down (Com-Sec responsibilities) – If **all** MDT's become inoperative, the shift supervisor shall contact Communications, and Communications will contact the System Administrator and the Special Projects Office. The System Administrator will make the determination if an immediate response is necessary, and will remedy the situation by whatever means, including contacting Atlantic Communications.

5. Routine maintenance – A regular maintenance schedule shall be maintained by the System Administrator. Officers will be notified when maintenance is due.

G. SECURITY:

1. Information obtained (NCIC/VCIN) –

a. The MDT will have a direct link to NCIC/VCIN. This system is a password-protected system and allows officers to access classified records. The protection of your password and the security of the MDT are critical to prevent unauthorized use of the NCIC/VCIN system.

b. The NCIC/VCIN system is to be accessed for **law enforcement purposes only** and is not to be used in violation of the 1972 Federal Privacy Act regarding the dissemination of criminal records to unauthorized persons. Personnel operating the MDT's will be held accountable for the protection of their respective password while accessing the system. Only authorized criminal justice personnel, while in the performance of their duties, are allowed access to the content(s) of any file retrievable through the computer. Whenever an officer accesses a file, the computer will create an audit trail of the transaction. This audit trail file can be accessed and can determine which files were accessed, the time they were accessed, and the individual who accessed the file.

c. Any access to NCIC/VCIN from a MDT is the responsibility of the operator whose password was used to log on the MDT. Any operator who allows unauthorized access, whether willfully or through negligence, is subject to disciplinary action and possible criminal prosecution.

d. Information from NCIC must be kept strictly confidential. Under no circumstances will any operator use another operator's password to gain access to the MDT system. Under no circumstances will any operator use any MDT logged on by another operator.

e. Any time a certified MDT operator feels his/her password has been compromised, it shall be reported to the System Administrator and a new password entered by the user. Unauthorized access will be considered a security violation and will subject the offender to departmental discipline.

f. Use of the MDT will be confined to the performance of an operator's official duties and subject to the same restrictions placed on radio transmissions. Radio and MDT transmissions are public record and subject to review.

g. While requesting information from NCIC/VCIN the information on the MDT screen should be restricted to the officer(s) only. Any unauthorized persons (suspects, victims, complainants, etc.) should not be allowed to view any information on the MDT screen. Confidentiality is very important and must be maintained at all times when dealing with any information in NCIC/VCIN files.

2. Password – Computer operators must use their individual password when accessing a MDT. Officers **shall not** share their password with any other individuals.

3. Mobile Data Terminal – Under normal circumstances (i.e. lunch break, etc.) officers shall close the cover, or blacken the screen of the MDT **every** time they exit their vehicle. Under no circumstances should the MDT screen be left visible when an officer is out of the unit on a complaint or away from the vehicle.

4. Out of vehicle – During an officer’s tour of duty, he/she will secure the vehicle every time he/she exits the unit by locking all doors and windows. Officers will be held accountable for damage to the computer and/or the vehicle if this procedure is not followed.

H. VERIFICATION OF NCIC/VCIN INFORMATION (Hit Confirmation):

1. A “hit” furnishes the officer with the fact that a stolen report, missing person report, or warrant has been filed. It also provides the date of theft, date missing, or date of warrant, which are matters to be considered by the receiving officer in arriving at an arrest decision. A hit is one fact that must be added to other facts by the officer in arriving at sufficient legal grounds for probable cause to arrest.

2. When an MDT operator receives a positive response from NCIC/VCIN and an individual is being detained, or a piece of property may be

seized, an immediate confirmation with the agency that originated the record in the system is necessary to ensure the validity of the hit before an arrest or seizure is made. To confirm a hit means to verify with the entering agency that the missing person report, theft, or warrant is still outstanding and that the person or property inquired upon is identical to the person or property listed in the wanted person, missing person, or stolen property record.

3. To initiate a hit confirmation, the MDT operator must notify the NCIC/VCIN terminal operator on the Information Channel by giving the exact data that was entered at the MDT to generate the original hit. The NCIC/VCIN terminal operator will resubmit the inquiry from the in-house terminal using the data supplied from the unit on the street. When the hit is received on the NCIC/VCIN terminal, the terminal operator will then contact the entering agency and verify the hit. Any information which is received by the terminal operator will be relayed to the MDT operator via the information channel. The MDT operator will then be responsible for using the verified information in establishing sufficient legal grounds for probable cause to arrest and/or seize property.

I. MDT Oversight Committee:

The Chief of Police will appoint a MDT Oversight Committee to review uses of and changes to the MDT program. This committee will meet on an as-needed basis.

J. MDT Inspections/Audit:

Random audits of Mobile Data Terminals will be conducted three times per calendar year. All Mobile Data Terminals, and any person that utilizes an MDT is subject to an audit. This audit will be conducted as part of the inspections process by the Professional Standards Branch.

-