NORTHAMPTON POLICE DEPARTMENT Administration & Operations Manual	
Policy: Use of Mobile Data Devices	**AOM: S-103**
Massachusetts Police Accreditation Standards Referenced: [41.3.7]	Issuing Authority ——————— Jody Kasper Chief of Police
Dissemination Date: 12/22/1998 **Effective Date:** 01/05/1999	**Amended:** 08/05, 09/08, 01/12, 01/15, 01/17, 1/19, 5/23 **Reviewed:** 06/02, 07/04, 08/05, 01/07, 01/09, 01/12, 1/19

Table of Contents

I. Introductory Discussion

The purpose of this directive is to provide department members with policy and procedures regarding the use of departmental mobile data devices.

II. Acceptable Use Policy

When using computers and communications equipment, services, and facilities, all Department personnel are expected to adhere to professional, ethical and lawful codes, and to use the equipment and facilities effectively and efficiently.

III. Procedures for Acceptable Use [41.3.7]

 A. All members of the Northampton Police Department shall adhere to the following procedures regarding the acceptable use of departmental mobile data devices:

1. Users agree to never use any part of the systems to perform illegal or malicious acts.
2. Users will not, on their own without proper authorization and support, alter their user access level or permission, attempt to access services not specifically allowed, deprive other authorized users of resources or access, or any way intervene in the operation and function of software, hardware, or services. Users will not alter the user interface, functionality, or capacity of the software or equipment, nor will they install or attempt to install additional software.
3. Passwords and other security login features assigned to each officer are not to be shared, and are the responsibility of each officer.

B. Mobile Data Terminals

1. At the start of the work shift, officers assigned to a vehicle equipped with a computer are required to log on the system and to immediately report any problems or defects in the system to the shift supervisor. Any failure of any part of the system during a shift shall be reported immediately to the Officer-in-Charge. Additionally, any problems should be documented on Fleetio.
2. During normal operations and functions, officers are instructed to stop their vehicles while sending or reading messages.
3. The vehicle computers are to be used only as terminals in the department's mobile data system. Nothing is to be attached to, placed upon, leaned against, connected to, inserted in, or otherwise made to impinge upon the machine, and the system is not to be used for purposes other than those for which it was specifically purchased. No software, other than that specifically authorized by the System Administrators is to be loaded into or used in the vehicle computers.
4. All communications are recorded, and may be reviewed by supervisors. These data records can be considered part of the public record and are subject to subpoena and other legal reviews.
5. Communications on the system shall be limited to that necessary for the performance of duty.
6. All information requested by an officer through the system shall be for official police use only.
7. Extreme care should be taken to avoid damage to mobile data computer equipment. Eating, drinking or smoking in the vehicle in a manner which results in damage will not be tolerated.
8. Officers shall logoff the computer at the end of their shift.

C. Mobile Data Devices

1. All members using any mobile device to include department issued cellular telephones, laptops, and or tablets, shall adhere to the same procedures listed above in Section III, subsection A, 1-4.

2. While utilizing any law enforcement only databases or applications on a mobile device they shall be for official law enforcement use only.