



East Norriton Township Police Department

GENERAL ORDER 7.1.17

RADIO, COMPUTER AND MOBILE DATA COMPUTER USAGE

Subject:

Issued Date:

March 23, 2011

Effective Date:

March 23, 2011

Revised Date:

July 11, 2018

PLEAC STANDARD Reference

Index Words

7.1.17 Radio, Computer and Mobile Data Computer Usage

A. Mobile and Portable Radios

1. Officers will ensure that the mobile and portable radio assigned to them is in working order. Officers will install a fully charged battery the portable at the beginning of the shift. Batteries shall be changed during the shift as necessary.
2. Any officer who damages the mobile or portable radio will be held responsible for the cost of repairs if it is shown that the damage was caused by the officer's negligence.
3. All officers while on duty will have their radios **ON** and set to **SCAN**.
4. Detectives will have a portable radio with them at all times while on duty, and outside of the police department building.
5. All other guidelines and rules set up by Montgomery County Emergency Services will be followed.

B. Computers and Mobile Data Computers (MDC's)

1. System Security:
 - a. All sworn and civilian East Norriton Police employees operating MDC's from a mobile unit, the PCO office or other location shall strictly observe regulations for such operations as set forth in policies, procedures and guidelines of the FCC, Montgomery County Communications Center, the Commonwealth Law Enforcement Assistance Network (CLEAN), National Crime Information Center (NCIC), and East Norriton Township Police Department.
 - b. All transmissions shall be in support of official law enforcement duties and responsibilities, and conducted in a professional manner.
 - c. No profanity, obscenity, prejudicial, derogatory, demeaning or unprofessional transmission will be broadcast on the MDC or radio system. This prohibition covers explicit text and/or implied violations of the previous described restrictions.
 - d. All information sent or received via the MDC system is **confidential**. Only authorized criminal justice agencies may request and receive this information.

- e. No officer or other member shall obtain or send information via computer and/or MDC system for purposes other than for official police investigation purposes.
- f. Every transmission whether sent or received via the MDC system is electronically recorded and is discoverable for court purposes. Members shall use discretion when sending messages. When records are subpoenaed these files will be included. In addition, all transmissions are subject to review.
- g. No officer or other member shall make changes in the system file and/or folder structures.
- h. No officer or other member shall install software, programs, screen savers, etc., without prior permission from police administration, with the exception of normal computer prompted upgrade requests.
- i. The MDC units shall be subject to periodic and unscheduled checks.
- j. Only trained members may use the MDC system.
 - 1.) Any officer or member required to use an MDC who has not been trained should notify the Lieutenant to obtain certification training.
 - 2.) Any officer or member required to use a MDC who does not feel qualified or confident in its use should not attempt to use the MDC, and should immediately notify their supervisor.
- k. Each member will be issued a user ID and PASSWORD to log on to the MDC system. All recorded transmissions will be assigned with the member's user ID. Members should safeguard their user ID and password to ensure the system's integrity.

2. Operational Security

- a. The MDC shall only be operated in a safe manner without endangering the operator, the vehicle, or other traffic.
- b. It is imperative that precautions be taken to safeguard the MDC equipment due to its value and its ability to access secure, confidential, criminal justice data.
 - 1.) The MDC must be locked in the docking station at all times.
 - 2.) The police vehicle must be locked whenever unoccupied.
- c. Officers must LOG OFF the MDC at the end of their shift.
- d. No Officer shall transmit on a MDC from another officer's vehicle or use a MDC logged in under another officer's password unless:
 - 1.) It is for a specific police purpose.
 - 2.) It is with the knowledge of the officer assigned that password or that vehicle.

3. Care and Maintenance of the Mobile Data Computer

- a. MDCs are expensive, sensitive electronic devices. Fluids, dirt and other foreign material will have an adverse effect in the operation of the MDC and its ability to function properly.
- b. Members are responsible to ensure that the MDC is in good working order at the beginning of their shift. If the MDC is missing, damaged, or not working, the member will immediately report this to his/her supervisor. If damage occurs during the shift, it shall immediately be reported to the shift supervisor.
- c. All malfunctions, damage, "dead spots", or other problems with the MDC's will be documented in writing and forwarded, through the supervisor, to the Lieutenant.
- d. Members shall not hang or place anything on or near the MDC. This restriction includes: food, beverages, clipboards, paperclips, microphones, cell phones, etc.

4. VIOLATIONS

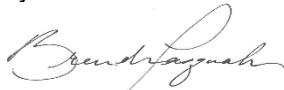
- a. Violations of this procedure or misuse of the MDC and its information is a security violation which will result in severe disciplinary action, punishable by the termination of the member's CLEAN/NCIC privileges, loss of MDC privileges, and the filing of criminal and/or civil charges by the Pennsylvania State Police.

5. CLEAN/NCIC HIT

- a. Any member receiving a positive hit on the CLEAN or NCIC system will verify all information through the Montgomery County Radio Room before taking any further action.

(Also see G.O. 1.4.5, 1.6.2, 1.6.3, & 1.6.5)

By order of:



Brandon Pasquale
Chief of Police