

		Policy & Procedures			No. 4.12	
		Subject:				
		Mobile Data Access				
		Issuing Authority:		Effective Date:	Review Date:	
		Chief of Police		10/30/2013	10/11/2023	
				Review Date:		
Review						
Revision	3/24/2014					
Reissued	9/30/2016					
	11/15/2018					
	02/13/2020					

41.3.7 11.5.1

GENERAL CONSIDERATIONS AND GUIDELINES

Computers are available to the Canton Police Department and Communications Center personnel to process information in a more efficient manner and to enhance the productivity of those using them. Computers are no more valuable than the information entered in them by the people who use them. They are available to officers, civilian employees and volunteers to accomplish our public safety mission.

We are becoming more and more dependent on computers. The door access system, records, MDT'S, communications consoles, property and evidence, mug shots, automated fingerprint system, Breathalyzer systems, telephones, crime analysis & mapping tools, surveillance equipment, traffic monitoring equipment, and even our heating and cooling systems in the facility rely on computers to function properly. Officers depend on them to document cases, produce reports, prepare presentations for citizens, and access information contained in our computers and those of other law enforcement agencies.

When computers fail, the ability of police to provide citizens with public safety services is compromised. When computers fail, the ability of police officers to receive vital information relative to their safety is compromised. Computers are acquired and maintained by the Canton Police Department to accomplish our police mission and not for personal amusement or personal business.

PROCEDURES

- I. The Chief of Police shall designate a person to be in charge of department computer systems. This person may designate other individuals who have responsibility for specific hardware and software within the department. These

individuals are responsible for the day to day operation and functionality of these systems.

- II. It is the responsibility of the person in charge of computer systems to act as a liaison with the Information System Department at the Town Hall in order to purchase, install, configure, and maintain police computer systems. Maintenance of computers is to be carried out only at the direction of this person or the Department Head of the IS Department.
- III. The shift commander on duty is responsible to assure that all police systems are in working order and to report all malfunctions to the proper person. The senior dispatching officer on duty is responsible to assure all CAD computers are in working order and to report all malfunctions pursuant to Communication Center directives to the shift commander. Depending on the severity of the breakdown and the necessity of the system to department operations the shift commander or senior dispatcher will determine if immediate notification is necessary or to wait until the person in charge is scheduled to work. Whenever any person with computer responsibility is working, they should be notified of the malfunction and given the opportunity to fix the problem if staffing allows.
- IV. All personnel will be issued passwords to the systems to which they are authorized. This password is confidential and should not be made available to any other person. When a person has reason to believe that their password has been compromised they will change it (if they have that ability) or request a new password from the person in charge of computer systems. Persons must use the password issued to them whenever using any computer system.
- V. All department computer systems are for business only. Examples of such systems would include portable laptops, mobile data terminals, tablets and cell phones to name a few. **41.3.7 (1A-D)** All employees are to refrain from installing software; including both unauthorized and unlicensed software **11.5.1**, modifying system setups, or attempting hardware or software changes or repairs unless they have received prior specific instructions from the person in charge of computers. **41.3.7 (3B)**
- VI. No hardware may be added to any department computer without the authorization of the person in charge of computers. **41.3.7 (3C)**
- VII. Programs, tables, and other files necessary for the operation of our Records and CAD systems will not be changed without the express consent of the person in charge of the computer system.
- VIII. Personal computers are issued to a person or bureau. No person may use these computers unless specifically authorized by the person in control of that computer or bureau. The configuration and initial settings on these computers may not be changed except with the knowledge and consent of the person in control of that computer, bureau or division.

- IX.** The person in charge of computers establishes regular backup routines for police reporting systems. Supervisors and employees should know if the work they do is covered by daily backup routines. Employees are warned that files stored only on local hard drives are not backed up. These files are the responsibility of the user and will be lost in the event of a hardware or software failure. Personnel using local hard drives must develop their own backup routines.
- X.** Internet access on department computers should only be utilized to accomplish the mission of the Canton Police Department.
- XI.** Internet connections are allowed only on those computers designated by the person in charge of department computers. Programs or other files may not be downloaded from the Internet nor will any information be transferred from on-line sources to any computer that is connected to our police reporting system. **41.3.7 (3B); 11.5.1**
- XII.** Storage devices and computer software from a non-secure source could corrupt the agency's computer system. Therefore, the following security protocol will be strictly adhered to: **11.5.1**
- There will be no installing any unauthorized or unlicensed software to any computer that is connected to our agency
 - There will be no transferring information from any source regardless of its origin (any data media source or drive)
 - There will be no transferring on information from on-line sources
- XIII.** Misuse of the LEAPS/NCIC computers may result in the Criminal History Systems Board disconnecting the department from the system. Unauthorized transactions and tampering with the hardware or software on this system is forbidden and will result in harsh disciplinary action. **41.3.7 (1B)**
- XIV.** Laptops installed in vehicles and the servers in the Communication Center are to be used only for police purposes. Unprofessional comments will not be transmitted from them. This department and other agencies keep a record of transmissions. No software may be loaded on this system without authorization of the person in charge of computers. Use of any disk or CD not authorized is strictly forbidden. **41.3.7 (3B)**
- XV.** Persons using any computer in the Canton Police Department will not access files or programs to which they are not authorized. Personal files, e-mail and other confidential files such as individual folders and documents are specifically for the use of person or persons designated to use them.

- XVI.** Information contained in Canton Police computers are for official police business. No person may disseminate information except as prescribed by law. It is a criminal offense to disseminate criminal offender information except as authorized by law. No information or database maintained by this department will be used for anything other than official police business except as specifically authorized by the Chief of Police.
- XVII.** Employees are warned that no right to privacy is to be expected or assumed when using police computer systems. Electronic mail and computer files prepared, displayed, started, transmitted, or received on Police computer systems could be viewed by the person in charge of computer systems or the Chief of Police or designee at any time.
- XVIII.** When using computers and communications equipment, services, all Department personnel are expected to adhere to professional, ethical and lawful codes, and to use the equipment and facilities effectively and efficiently.
- A. Canton Police Department personnel shall never use any part of the system(s) to perform illegal or malicious acts.
 - B. Canton Police personnel shall 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; including both unauthorized and unlicensed software. **41.3.7(3C); 11.5.1**
 - C. 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 shift supervisor, and a defective equipment/system form will be completed and forwarded to officer(s) serving as system administrator.
 - D. During normal operations and functions, officers should stop their vehicles while sending or receiving messages. All officers are advised to fold down the screen while driving their vehicles to avoid dangerous distractions. The laptop computer will provide an audible alert when an incoming message has been received; the screen does not need to be visible for an officer to know when information requests or notifications have been received.
 - E. 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.
41.3.7(1B)

- F. Communications on the system shall be limited to those necessary for the performance of duty.
- G. Passwords and other security login features assigned to each officer are not to be shared, and are the responsibility of each officer.
- H. 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.
- I. All information requested by an officer through the system is for official police use only.
- J. Extreme care should be taken to avoid damage. Eating drinking or smoking in the vehicle in a manner which results in damage will not be tolerated.
- K. Officers will logoff at the end of their shifts.