TOWN OF SENECA FALLS POLICE DEPARTMENT

GENERAL ORDER

GENERAL ORDER #: 510	**RESCINDS:**
SUBJECT: Computer and Electronic Messaging	**NYS ACCREDITATION:** 55.5
EFFECTIVE DATE: 04/17/2018 **BY ORDER OF:** Stuart W. Peenstra, Chief of Police	

I. **PURPOSE:** The purpose of this order is to establish policy and procedures regarding the use of department computer and electronic messaging systems.

II. **BACKGROUND:** The availability and use of computers in law enforcement has provided many opportunities for the enhancement of productivity, investigative effectiveness, and officer safety. While increased access to information has benefited our department, technology that entails easy access to and the rapid transfer and distribution of sensitive data has the potential to have a damaging effect on the agency, our members, and the public if not managed properly.

III. **POLICY:** It is the policy of the Town of Seneca Falls Police Department that all members shall abide by the guidelines established for the use of department computers to include applicable department rules and regulations, other department written directives, interface provider (e.g., Integrated Justice Portal, SPILLMAN, BIOMETRICS) regulations, directives, operating instructions, use and dissemination agreements, and all applicable federal and state statutes.

IV. **DEFINITIONS:**

A. **DEPARTMENT COMPUTER:** Any personal computer, laptop computer, dumb terminal, hand-held computer device, wireless computer device, or similar device owned, leased, operated, or maintained by the Town of Seneca Falls Police Department.

B. **AUTHORIZED USER:** Any member of the department authorized by appropriate authority to utilize a department computer(s).

C. **NETWORK ADMINISTRATOR:** The Network Administrator responsible for managing the department's personal computer Local Area Network (LAN) to include related hardware and software is not a member of the Seneca Falls Police Department.

D. **TERMINAL ACCESS CONTROLLER (TAC):** The member of this agency designated by the Chief of Police with the responsibility for managing the department's participation in the Integrated Justice Portal and SPILLMAN/CAD criminal justice information systems, Leads Online, to include insuring compliance with applicable policy, rules, regulations, and operating instructions.

E. **NY INTEGRATED JUSTICE PORTAL:** New York State Integrated Justice Portal to include messaging and database inquiry (e.g., DCJS, NCIC, DMV).

F. **SPILLMAN:** Seneca County's Incident Reporting System to include arrest and incident

Reporting/records management, help files, and the computer-aided dispatch (CAD) interface.

G. TraCS: Traffic and Criminal Software system is an electronic method of issuing traffic citations and reporting accidents.

H. LeadsOnline: Investigative Tool consisting of online searching of nationwide second Hand transactions that are reported to Leadsonline.com (ie. Pawn shops, jewelry stores etc.)

I. TLO: Investigative tool that consists of online searches of names, phone #'s etc.

J. UNAUTHORIZED SOFTWARE: Any software that has not been approved by the Chief of Police or Network Administrator and licensed for use on department computers or electronic device. This includes any software not required for job related duties.

K. DOWNLOADS: Copies of computer files obtained through removable media (e.g., USB drive, floppy disk, zip disk, CD ROM) or received from another computer or the internet.

V. PROCEDURE:

A. GENERAL USE AND PRIVACY

1. The use of any department computer is authorized for official business only and is considered a privilege subject to revocation.

2. Members do not maintain any right to privacy when using a department computer and its contents, to include personally owned software. By using a department computer, all members knowingly and voluntarily consent to electronic monitoring and acknowledge the department's right to conduct such monitoring. The department reserves the right, without notice, to:

    a. Access any information composed, created, received, downloaded, retrieved, stored, or sent using department computers.

    b. Access, for quality control, audit, or internal affairs purposes, any electronic messages generated by members utilizing department computers.

    c. Require members to provide passwords to systems or files that have been password protected or encrypted.

3. Accessing or transmitting materials other than for official police business that involves indecent, sexually explicit, and/or unprofessional language or images, or that disparages any person, group, or classification of individuals is prohibited.

4. Installation of and access to software of a purely entertainment use (e.g., computer games) is prohibited.

B. SECURITY AND CONFIDENTIALITY

1. The use of department computers shall be limited to legitimate law enforcement purposes and department communications.

2. All information stored within or accessible by department computers shall be treated as confidential information and may only be accessed, disclosed and disposed of in accordance with department policy and procedures, the policy, rules, regulations, operating instructions, and/or the use and dissemination agreements of information provider agencies, as well as all other applicable federal and state laws.

3. Only authorized users may use department computers. Members assigned to use a department computer will be responsible for maintaining its physical security as well as the integrity and security of data contained therein. Every reasonable precaution available shall be used to safeguard the computer/data (e.g., locking unattended police vehicles, logging-off terminals when leaving a computer unattended, shielding screens from public view, maintaining password confidentiality).

4. No member will access or attempt to gain access or allow an unauthorized person to gain access to any department computer or any area of a department computer or network that he/she is not authorized to access. This includes, but is not limited to, hardware drives, network drives, interfaces, removable media, software program, databases, and mailboxes.

5. Members viewing any information on department computers are responsible for the security and confidentiality of that information. Information and reports viewed in electronic form are considered the same as printed material. All applicable policies and procedures, regulations, use and dissemination agreements, and laws governing the release and disposition of computer information shall be followed. Confidential printed information should be shredded.

6. Confidential, proprietary, or sensitive information may be disseminated only to authorized persons with a need and a right to know and only when there is sufficient assurance that the appropriate security of such information will be maintained. Examples of such information include, but are not limited to:

    a. Personnel information such as personnel complaints, performance reviews, internal investigations, grievances, disciplinary information, personal employee information, and medical records.

    b. Internal department memorandums or communications.

    c. Criminal history information and any other files protected by law (e.g., juvenile delinquency records).

    d. Confidential informant, intelligence, and identification files.

7. Members are required to immediately report any potential, suspected, or

known breach of department computer security to the Chief of Police, Lieutenant, TAC, or Network Administrator.

C. TRAINING AND CERTIFICATION

1. All authorized users shall receive appropriate training regarding the department computer systems they are authorized to use:

    a. The Network Administrator or his designee will be responsible for providing training regarding the department's personal computer LAN, office software, and utilities.

    b. The TAC will be responsible for providing training and operator certification in regard to the Integrated Justice Portal computer systems.

    c. The Field Training Officer (FTO) will be responsible for ensuring that members receive training in regard to the MCT system, Spillman and TraCS system.

2. Additional computer training and certification requirements as well as operating procedures will be provided as required and or needed.

D. PASSWORDS

1. Access to department computers and networks shall be password controlled. The Network Administrator or his designee will be responsible for assigning password access to the department's LAN, and TraCS. The TAC will be responsible for establishing password access to SPILLMAN, LEADS ONLINE and the Integrated Justice Portal computer systems.

2. Passwords shall be selected so as they are not easily guessed. Whenever practical, they shall include a combination of letters, numbers, and symbols.

3. It is strongly recommended that passwords should be changed at least once per year.

4. Members shall not give their passwords in any discernible form (written or verbal) to anyone else except as provided in this directive (e.g., directed by command or computer support personnel for business or maintenance purposes). Written passwords or access codes shall not be left in or near computers.

5. Members shall not use any password other than their own.

6. Password holders will be held accountable for computer access gained through use of their assigned password.

7. No member shall permit an unauthorized person to use the departments Computer system.

8. If a member leaves the department's employment, suspended from duty, absent for a prolonged period of time, or is no longer authorized to access any component of the department's computer system, his/her supervisor shall

notify the Lieutenant who shall direct deactivation of the appropriate password account(s).

E. SYSTEM ADMINISTRATION

1. The Network Administrator or his designee is responsible for the installation, maintenance, support, repair, operation, and security of all department computers with the exception of the security, data integrity, and operational duties assigned to the TAC pursuant to SPILLMAN, TRACS, LEADS ONLINE, BIOMETRICS and the Integrated Justice Portal rules and regulation.

2. Requests for maintenance, support, or repair shall be accomplished via the SFPD "Equipment Repair Form" Requests requiring capital expenditures, major system impact, or substantial commitment of resources shall be directed through the chain of command.

3. Members may not add or modify hardware or software to department computers, or adjust hardware settings (to include computer systems, printers, scanners, modems, and monitors) unless specifically authorized by the Chief of Police, Network Administrator or their designee. In addition, members are prohibited from:

    a. Taking apart or removing external cases.

    b. Altering system files.

    c. Uninstalling, removing, or altering agency owned programs.

    d. Removing system batteries.

    e. Swapping system parts.

4. No unauthorized software may be installed on department computers. Privately owned software may be installed if approved by the Chief of Police. Such software may be removed if it conflicts with department hardware or software or occupies excessive storage space.

5. Members shall observe the copyright and licensing restrictions of all software, documents, images, or sound and only licensed software may be installed on department owned computers. Any software for which proof of licensing (i.e., original disks, original manuals, and/or license) cannot be provided is subject to removal by the Chief of Police, Network Administrator or their designee.

6. System users shall take the necessary anti-virus precautions before accessing any external media or downloading or copying any file from the Internet. All media and download files are to be checked for viruses; all compressed files are to be checked before and after the files are decompressed. Suspected viruses shall be isolated and reported to the Chief of Police, Network Administrator or their designee.

7. Members shall be responsible for the basic care, maintenance, and operation of department computers to include:

a. Following proper power-up and shut down protocol.

b. Preventing exposure to food, liquid, or other damaging elements.

c. Preventing damage or mistreatment.

d. Removing any device that may potentially damage the system.

e. Updating and maintaining the integrity of system passwords.

f. Following applicable instructions and procedures.

g. Notifying the Network Administrator or TAC of any malfunctions or other system anomalies.

8. To avoid breach of security, members shall log off any department computer or any other computer that has access to the department's computer system (to include, Email, SPILLMAN, Integrated Justice Portal, LEADS ONLINE, TraCS, or Internet) whenever they leave their workstation.

F. SYSTEM PROTECTION, DATA BACK-UP AND STORAGE, AND AUDIT

1. The Network Administrator or his designee is responsible for the administering the department's anti-virus and system protection program to include:

   a. Loading and maintaining virus and firewall protection on all department owned personal computers and network drives.

   b. Timely update of virus definition files.

   c. Disseminating information regarding the use of utilities which safeguard department computers (e.g., virus scan, firewall software, file backup).

   d. Isolating detected viruses and system intrusions and minimizing damage.

   e. Recovery efforts following attacks.

2. The Network Administrator or his designee shall be responsible for establishing and ensuring back-up procedures and for the regular backup of data stored on the department's LAN server. System users are responsible for any data not stored on a network drive. Storage and retention will be in an appropriate and secure manner and where applicable be in compliance with the NYS Records Retention and Disposition Schedule (MU-1).

3. The Chief of Police shall maintain a liaison with the Seneca County Department of Emergency Communications, Seneca County Department of Information Technology, and the New York State Police to insure the proper back-up and storage of central records system data to include, TraCS, SPILLMAN arrest and incident records.

4. To insure the integrity of the department's central records computer system, the Chief of Police or his designee shall perform an

annual audit of the system for verification of passwords, access codes, or access violators.

G. ELECTRONIC MESSAGING (LAN, INTERNET, PAGING)

1. Electronic messaging through department owned computers or radio pagers is designed to enhance our efficiency. The use of electronic messaging shall be limited to legitimate law enforcement needs and department communications.

2. Since LAN e-mails have become a primary method of communications within the department, members are required to check their LAN e-mails at the beginning of each shift. **(55.5)**

3. All messaging that is composed, transmitted, or received via our computer systems is considered to be part of the official records of the department and, as such, is subject to disclosure to other third parties. Consequently, members shall always ensure that information contained in messaging is accurate, appropriate, ethical, and lawful.

4. The following types of electronic messages are specifically prohibited:

    a. Sending or posting confidential or sensitive information to those not authorized to receive it.

    b. Sending or posting material that could damage the department's image or reputation.

    c. Distributing copyrighted materials without the consent of the copyright owner.

    d. Sending or receiving messages for personal gain or non-department business.

    e. Sending or posting material that is discriminatory, harassing, or obscene, or for any other purpose that is illegal, against department policy, or not in the best interest of the department.

    f. Misrepresenting your identity.

    g. Any activity that tends to clog the system to include sending or forwarding chain letters, unnecessarily sending messages to a large number of recipients, unnecessarily large attachments, or using excessive storage space on message servers.

5. In order to limit the resources needed to store electronic messages, the department reserves the right to delete stored messages. Information that needs to be saved should be printed and filed in the appropriate place.

H. MOBILE COMPUTER TERMINAL (MCT) SYSTEM

1. The Seneca County Department of Information Technology shall be responsible for the administration of the department's Mobile Computer Terminal (MCT) system. He/She will be assisted by the following personnel:

   a. The Chief of Police or his designee who will administer MCT hardware and software applications; and

   b. The TAC who will administer CAD password access, certification and training.

2. In addition to the guidelines and procedures promulgated in this directive and other applicable general orders, the following directives shall apply specifically to MCT operation:

   a. Members shall inspect their MCT at the beginning and end of their watch for any defects, damage, or operating problems. Problems shall be reported to the Shift Supervisor without undue delay, and an electronic "Equipment Repair Form "shall be submitted detailing the problem or issue.

   b. No member shall type on or read a MCT while the vehicle is in motion, unless the member is certain the operation performed will not distract his attention from the safe operation of the vehicle. Drivers utilizing MCT's should stop their vehicle in a safe manner before attempting to access information.

   c. Equipment in the interior compartment of police vehicles shall be secured to prevent striking the MCT or the officer during an abrupt stop. MCT's shall not be used as a worktable or for equipment storage and liquids or food products shall not be placed on or near the MCT. If a liquid is spilled on an MCT, turn the unit off and bring it into headquarters. Dry the keyboard off and notify the Shift Supervisor and the Lieutenant.

   d. MCT messaging transmissions are stored in the CAD mainframe system for extended periods of time and are considered public records, available through the Freedom of Information Law (FOIL). MCT messaging shall be limited to legitimate law enforcement needs and department communications. The Chief of Police shall assign a supervisor to conduct period reviews of MCT traffic to ensure that the system is being used in an appropriate manner.

I. INTERNET ACCESS

1. The department may at its discretion provide members with Internet access to e-mail and/or information on the World Wide Web or similar data collection technology. Access is provided for department business use only.

2. Internet access shall be done in a professional manner in compliance with all applicable laws and department policies, and as authorized by the member's

Supervisor. The Internet shall not be used for any illegal, improper, unprofessional, illicit, or non-official business.

3. The Internet is a valuable tool and members may use the Internet in the performance of their duties to enhance their effectiveness. Users should not be “surfing the net” during work hours.

4. All files downloaded from the Internet shall be downloaded to the user’s local hard drive (:H\) and scanned for viruses prior to being opened on any department computer. No files should be copied to any network drive unless the files have been scanned for viruses.

5. No Photographs are to be stored on the department computers unless authorized by the Chief of Police or his designee.

6. No videos are to be stored on the department computers unless authorized by the Chief of Police or his designee.

5. As with all department computer use, the department reserves the right to access and review Internet use on department computers as necessary to ensure that there is no misuse or violation of department policy or any law. The Network Administrator or his designee will monitor Internet activity and shall report abuse to the Lieutenant.