Subject: **Computer Use & Electronic Messaging**
Policy #: **301.3**
Effective Since: 8-21-03
Revision Effective: 1-1-19 FTO Training Task: # 11
Reference Material: IACP "Electronic Messaging" Research Paper
ILEAP Standards Covered: NA **Page 1 of 3**

PURPOSE: It is the purpose of this policy to provide employees with guidance on the proper use of personal electronic devices, computers, and related electronic messaging systems utilized in this agency for purposes of disseminating messages, electronic mail, utilizing services of the Internet and related electronic message transmission, recording, and storage devices.

POLICY: The availability and use of the personal computer and personal electronic devices within the work environment has provided many opportunities for enhancement of productivity and effectiveness. These technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this agency, its members, and the public if not managed properly. Therefore, it is the policy of this agency that all members abide by the guidelines set forth herein when using personal computers, personal electronic devices, and the services of both internal and external databases and information exchange networks, and where applicable, voice mail, mobile data terminals, and related electronic messaging devices.

DEFINITIONS:

Electronic Communication Device (ECD): For purposes of this policy, electronic communication devices include personal computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards, internet services, mobile data terminals, text messaging, social media messaging, other electronic messaging apps, and facsimile transmissions.
System Administrator: For purposes of this policy, the member of this agency designated with responsibility for managing all aspects of electronic messaging through individual computers and computer networks within this agency. The system administrator is the Commander in charge of Records, or their designee.
LEADS: Law Enforcement Agency Data System.

PROCEDURES:

A. **General Use and Electronic Messaging** :

1. Transmission of electronic messages and information on communications media provided for employees of this agency shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence.
2. Information contained in electronic messages of any type shall not be released to anyone outside the department without prior approval of the Chief of Police.
3. This agency encourages authorized and trained personnel with access to ECD's to utilize these devices whenever necessary. However, use of any of these devices is a privilege that is subject to revocation.
4. ECD's and their contents–with the exception of personally owned software authorized for installation on agency computers–are the property of this agency and intended for use in conducting official business with limited exceptions noted elsewhere in this policy.
5. Members are advised that they do not maintain any right to privacy in ECD equipment or its contents, to include personally owned software.
    a. This agency reserves the right to access any information contained in ECD's and may require members to provide passwords to files that have been encrypted or password protected.

   b. The agency reserves the right to access, for quality control purposes and/or for violations of this policy, electronic and voice transmissions of members conducting business of this agency.
6. Accessing or transmitting materials (other than that required for police business) that involves the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.
7. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or networked systems) only to individuals with a need and legal right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes but is not limited to the following:
   a. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information.
   b. Criminal history information and confidential informant master files, identification files, or related information.
   c. Intelligence files and information containing sensitive tactical and undercover information.
8. No member shall access or allow others to access any file or database unless that person has a need and a right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.
9. Employees with LEADS certification and access are further governed by the rules, regulations, and procedures established by LEADS. No employee shall use LEADS without requisite certification and/or in violation of any LEADS regulations.
10. An ECD is designed and intended to conduct business of this agency and is restricted to that purpose. Installation of or access to software for purely entertainment purposes is prohibited. Exceptions to business use include the following:
    a. Infrequent personal use of these devices may be permissible if limited in scope and frequency, if in conformance with other elements of this policy, and if not connected with a profit-making business enterprise or the promotion of any product, service, or cause that has not received prior approval of this agency.
    b. Personnel may make off-duty personal use of agency computers for professional and career development purposes when keeping with other provisions of this policy and with prior knowledge of an appropriate supervisor.
11. Personnel should not, without permission from the System Administrator, make any changes, alterations, manipulations, or additions to computer hardware devices or software configuration settings.
12. Malfunctions with any department computers or related equipment or software should be brought to the attention of a supervisor, who can forward the information to the System Administrator. Unauthorized personnel shall not attempt physical repair of any computerized equipment, though employees may engage in ordinary rebooting and troubleshooting attempts when necessary.

B. **Importing or Downloading Information and Softwar e**

1. Members shall not download or install on their personal computer or network terminal any file (including sound and video files and files attached to e-mail messages), software, or other materials from the Internet or other external sources without taking prescribed steps to preclude infection by computer viruses. Such downloading is subject to approval by the System Administrator.

   a. Material shall be downloaded to secure storage drives and scanned for viruses prior to being entered into any personal or shared system.
   b. In no case shall external materials or applications be downloaded directly to any shared (network) drive. When in doubt, members shall consult the system manager for guidance.
2. Members shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.
   a. Any software for which proof of licensing (original disks, original manuals and/or license) cannot be provided is subject to removal by authorized agency personnel.
   b. Privately owned software may be loaded on agency computers only if approved by the System Administrator.
   c. All original license of privately-owned software must be maintained with the System Administrator after approval of such installation.
   d. Privately owned software may be removed if it conflicts with departmental hardware or software, interferes with the ability of other members to access or utilize the ECD, or occupies excessive storage space needed by the agency.
3. Members shall observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.
4. Any hardware enhancements or additions to agency-owned equipment must be approved and authorized by the system administrator. The system administrator is responsible for determining proper installation procedures.
5. Members shall not permit unauthorized persons to use any department-owned ECD.
6. To avoid breaches of security, members should log off, or electronically "lock" any personal computer that has access to the agency's computer network, electronic mail system, the Internet, or sensitive information whenever they leave their workstation **and** when such information could readily be viewed or used by an unauthorized person. Access to personal computers should be protected using the computer's internal security measures such as automatic locking of workstation after a predefined period of time, preferably after 15-20 minutes.

Policy originally issued 8-21-03; this revision becomes effective on 1-1-19 by authority of the Chief of Police .

NOTE: This policy and procedure summarizes the department's position on this specific matter. This policy is for general direction and guidance primarily designed for use by the department's members. This policy is for internal use only and does not create or enlarge an officer's liability in any way. This policy shall not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this policy, if proven, can only form the basis of an internal departmental complaint and then only in a non-judicial administrative setting.