KENOSHA POLICE DEPARTMENT

POLICY AND PROCEDURE

81.4 Electronic Communications

Effective Date:	12/1/2000	**Revision Date:**	9/5/2008
Action:		**Number of pages:**	5

I. PURPOSE

The purpose of this policy is to provide the officers and civilian employees of the Kenosha Police Department with guidance on the proper use of electronic messaging devices such as Personal Computers, Mobile Data Computers and Facsimile Machines utilized by the department for the purpose of disseminating electronic mail, utilizing services of the Internet and related electronic message transmission such a Voice Mail, electronic pager systems, recording and storage devices.

II. POLICY

The availability and use of the personal computer and Electronic Messaging Devices (EMD) within the Kenosha Police Department have 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 department, its members, and the public if not managed properly. Therefore, it is the policy of this department that all members abide by the guidelines set forth in this policy and General Ordinance 1.30 of the City of Kenosha when using personal computers, the services of both internal and external databases, information exchange networks, and where applicable, voice mail, mobile data computers, telephones, cell phones, and related electronic messaging devices. All uses of Electronic Messaging Devices will be treated with the same degree of propriety, professionalism and confidentiality as official written correspondence or public records.

III. DEFINITIONS:

Electronic Mail (e-mail):
Communications sent to or received from any person whether or not a department employee, through a department computer including information sent or received via the Internet.

Electronic Messaging Device (EMD):
For the purpose of this order, Electronic Messaging Devices include personal computers, electronic mail systems, voice mail systems, paging system, electronic bulletin boards, Internet service, telephones, cell phones, mobile data computers and Facsimile transmissions.

Internet:
The collective myriad of computer and telecommunications facilities, including equipment and operating software, that comprise the interconnected worldwide network that employ transmission control protocol or Internet protocol, or any predecessor or successor protocols or technologies, to communicate information of all kinds by wire or wireless Transmission.

Local Area Network (LAN): A network allowing computers or locals computing units to exchange information with other computers and share resources.

LAN Coordinator:
An individual, who has been trained and appointed to assist the System Administrator with computer related problems and coordinate support for the systems.

Login Name:
A user name derived from the first letter of the employee's first, middle and last name followed by the employee's unit number (ABC123).

Login Password:
A unique password that is used by an individual to log in and gain access to a computer system in conjunction with the Login Name.

Mobile Data Computer (MDC):
A lap top computer system that is owned by the City of Kenosha Police Department, equipped with a radio modem and used by employees to communicate information to and from remote sites.

Personal Computer System (PCS):
A personal computer system that is owned by the City of Kenosha, Kenosha Police Department or Kenosha City/County Joint Services and assigned to an individual or work station, Division or Unit.

System Administrator:
An employee assigned by the Chief of Police designated with the responsibility for managing all aspects of electronic messaging through individual computers and computer networks within the Kenosha Police Department.

Work product:
Any document, spreadsheet, program or other electronic files that are created or produced on a PCS.

IV. PROCEDURE

A. General

1. Electronic Messaging Devices (EMDs) and their contents including work products are the property of the Kenosha Police Department and intended for the use in conducting official business with limited exceptions noted elsewhere in this order.
2. This department encourages authorized personnel with access to EMDs to use these devices whenever necessary.
3. Transmission of electronic messages and information on communication media's provided for the members of the Kenosha Police Department shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence or public records.
4. Members of the Kenosha Police Department are advised that they do not maintain any right to privacy in EMD equipment or its contents including personally owned software.
    a. The department reserves the right to access any information contained in the EMDs and may require members to provide passwords to files that have been encrypted or password protected.

b. The department 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 department. This includes but is not limited to personal e-mail, voice mail, notes, documents, files and system accounts.

5. 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.

6. The Internet shall be used for law enforcement purposes only. The transmission of any material in violation of any City, State or Federal law or regulation is prohibited.

7. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories on the networked system) only to individuals with a need and a right to know and when there is sufficient assurances 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, juvenile record information and confidential informant master files, identification files, and 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.

   a. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.

   b. No one is to operate any network/system terminal while utilizing a password or access privilege not assigned to him or her.

   c. Members shall not permit unauthorized persons to use this agency's electronic mail system.

   d. To avoid breaches of security, members shall log off or lock (if gone temporarily) any personal computer that has access to the agency's computer network, electronic mail system, and Internet, or sensitive information whenever they leave their workstation.

B. Importing / Downloading Information and Software

1. Members shall not download or install any file (including sound and video files attached to e-mail messages), software, executable files, or other materials from the Internet or other external sources without the approval of the system administrator and take prescribed steps to preclude infection by computer viruses.

2. Members shall observe the copyright and licensing restrictions of all software 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 not be loaded or run on agency computers without approval of the System Administrator.

3. Members shall observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.

C. Hardware

1. 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.

2. Disassembling of computer components/workstations is prohibited unless performed as maintenance, repair or upgrade by authorized personnel. This section does not apply to personnel trained for the purpose of replacing disposable items such as printer paper, ribbons and ink or toner cartridges.

3. Computer components will not be unplugged, reconfigured, or moved from their original location without prior approval and assistance of trained personnel.

   a. Personnel will not configure, modify, partition, or alter any predefined hardware or CMOS/MOS setting, hard disk, or software configuration located in any system CONFIG.SYS or AUTOEXEC.BAT files.

   b. No hardware attached to any department personnel computer or laptop computer will be disconnected without the permission of the system administrator or personnel having the authority to authorize the disconnection of the hardware.

4. Any damage or malfunction of computer components/workstations shall be reported to the system administrator, LAN coordinator, or other appropriate supervisor immediately so that corrective action can be taken.

D. Network Operations

1. Personnel who have called for an application but are not actively using such application are required to exit the program. This will allow others to utilize the application such as Attendance Records and some CISCO files, which only allow one user at a time.

E. Responsibilities

1. Shift Commander Responsibilities

   a. Review his/her internal email in Outlook repeatedly while on duty.

   b. Ensure that subordinate supervisors review their email in Outlook at least daily.

   c. Disseminate critical information received on email to the appropriate subordinates.

   d. Respond to all email needing a response on a timely basis.

   e. Monitor and review MDC messages at least once a month.

2. Supervisor Responsibilities

   a. Review his/her internal email in Outlook at least daily.

   b. Ensure that subordinates review their email at least daily.

   c. Disseminate critical information received on email to appropriate subordinates.

   d. Respond to all email needing a response on a timely basis.

3. Officer Responsibilities
    a. Review his/her internal email in Outlook at least daily.
    b. Respond to all email needing a response on a timely basis.

4. Civilian Employees Responsibilities
    a. Review his/her internal email in Outlook daily.
    b. Respond to all email needing a response on a timely basis.

V. TRAINING

Each member of the Kenosha Police Department shall receive training on this policy and the operation and function of the various Electronic Messaging Devices and Personal Computer Systems that the employee may be required to work with during his/her term of employment. If an employee feels they do not have the necessary ability or knowledge to operate these devices or systems they shall be responsible to request assistance and additional training.