KANSAS CITY, MO. POLICE DEPARTMENT **PERSONNEL POLICY**	DATE OF ISSUE 02-09-10	EFFECTIVE DATE 02-09-10	NO. 260
SUBJECT **Policy Series 200: Employee Guidelines** **260 - Computer Use and Security**		AMENDS	
REFERENCE RSMo. 569.094; 569.095; 569.097; and 569.099 PPBM: 330, "Department-Owned Equipment-Privacy and Security"		RESCINDS PI: 01-8 DM: 02-28 ABM: 08-4	

I. PURPOSE

To provide instructions for members regarding computer systems, electronic mail (e-mail), and Internet usage.

II. POLICY

The security of the department's computer system is of paramount importance in maintaining an efficient and well-guarded database for referencing computerized information. Users will strictly adhere to the following guidelines on the usage of department computers and associated software to ensure compliance with federal copyright laws and protection against computer viruses.

III. TERMINOLOGY

A. **Breach** - A break in the system security that results in admittance of an unauthorized person or program to a department computer system.

*B. **Electronic Mail (E-mail)** - A system for sending and receiving messages electronically over a computer network accessed through a department owned computer.

C. **Firewall** - A system (hardware or software) designed to prevent unauthorized access to or from a private network.

D. **Hardware** - The physical computer system or any physical part or mechanism used as an integral or peripheral component of a computer system, e.g., a floppy or hard drive mechanism, memory modules, display monitor and interface card.

E. **Intranet** - Uses Internet based technologies within an organization to facilitate communication and provide integrated access to information.

F. **Internet** - A worldwide network of computers linked together by various communication systems including local telephone services.

*G. **Network** - A system of computers, printers, and storage devices linked by direct connection, over data circuits, fiber optic lines or via other electronic transmission methods that allows shared access to all resources on the network.

*H. **Malware** - Short for "malicious software," malware refers to software programs designed to interfere with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

*I. **Microsoft Outlook** - A software application used to create, receive, transmit, store, and archive E-mail messages as well as store calendar, tasks and contact information.

*J**.** **Tiburon** - The vendor contracted to provide records management, corrections management, automated field reporting and computer aided dispatching software applications for the Police and Fire Departments.

*K. **Software** - The programming instructions the computer executes to perform tasks.

1. **Freeware Software** - Software freely obtained from public sources.

2. **Shareware Software** - Software obtained through public sources with normally limited features, periodic visual reminders to purchase, or a time limit cutoff to prevent use without purchase.

3. **Open Source Software** - Computer software whose source code is available under a license or arrangement such as the public domain that permits users to use, change, and improve the software, and to redistribute it in modified or unmodified form.

4. **Commercial Off the Shelf Software (COTS)** - software that is purchased from a retail outlet and installed to the user's computer.

***L. **Unauthorized Equipment or Software** – Equipment or software that has not been provided by the department or is not properly licensed to the department.

M. **Virus** - A self replicating computer program capable of attaching itself covertly to files. Can also be an executable program designed to perform actions not authorized by the system's user.

*N. **Virtual Private Network (VPN)** - A private communications network often used by companies or organizations to communicate confidentially over a public network.

O. **Worm** - A computer program designed to covertly destroy or manipulate data, but cannot attach itself to other programs. A worm still replicates itself to other computers and uses memory, but will always arrive in the same program.

IV. ADMINISTRATIVE GUIDELINES

A. These procedures apply to all members of the Kansas City, Missouri Police Department utilizing department computer equipment or department computer systems. Use of these systems implies that members agree to comply with all applicable policies, guidelines and laws regarding their use.

B. Only the Information Technology Division or its designee will install hardware/software on department computers, with the exception of those elements which have an authorized network administrator.

C. The Information Technology Division is responsible for granting and monitoring access to department computer systems by issuing each department member a User ID. Members are prohibited from using any User ID which is assigned to another person. Members needing assistance acquiring User ID and/or password are directed to contact the Computer Help Desk.

D. Members are responsible for access to and use of their User ID and password, regardless of who actually uses it; therefore, members are responsible for logging off the network upon completion of their computer activity and locking their workstation.

E. Members may not alter or copy a file belonging to another user unless they need to access those files in the performance of their duties.

F. Members may not use the department computer systems to invade the privacy of other department members by unnecessarily reviewing their files and e-mail.

G. Members will not interfere with or disrupt any department computer system, Internet user, program, or equipment. Disruptions include but are not limited to propagation of computer worms, viruses, or other debilitating programs, and using the department computer system to make unauthorized entry to any other machine accessible via the computer system or Internet.

H. Each member is responsible for taking reasonable precautions to avoid introducing viruses, worms and malware to department computer systems and notifying the Computer Help Desk if a virus has been introduced to the network.

*I. Files saved to the Public Drive (P:\Public Drive) on the network should be backed up. Anyone on the network has access to that drive and has the ability to delete the files located on that drive.

*J. No unauthorized equipment will be attached to the network.

K. The Department reserves the right to access, view and copy any user's electronic communications messages, files, data, correspondence, log files, etc. created by or stored on a Department owned electronic communication system or device. The Department reserves the right to use the data and/or content for any purpose.

V. TABLE OF ANNEXES

James D. Corwin
Chief of Police

Adopted by the Board of Police Commissioners this _____day of _____, 2010.

Mark C. Thompson
President

DISTRIBUTION: All Department Personnel
Post on Bulletin Boards for two weeks
Public View Master Index - Internet
Department Master Index - Intranet

DEPARTMENT OWNED COMPUTER EQUIPMENT

A. The use of software/hardware on department computers will be limited to lawful and productive endeavors.

B. The handling of any computer software will be as follows:

1. The unauthorized copying of department computer software is prohibited.

2. Copies of the registration and/or license agreement will be forwarded and maintained in the Information Technology Division.

3. All shareware, freeware and COTS software must be reviewed by the Information Technology Division prior to being installed on any department computer.

C. Only Information Technology Division personnel, or an approved designee, will move, install or disassemble department computer equipment.

*D. Members will not use privately owned personal computer equipment for department business through a VPN to access the department secure network to access department computer applications or servers without prior approval from the Information Technology Division.

E. Privately owned computers will not be connected to the department's secure network.

*F. Non-Department Members Access to the KCPD network or computer applications.

1. When non-department personnel (e.g. members of a task force, special assignment or internships) need access to the KCPD network, the element overseeing this individual (responsible element) shall forward the individual's information through the chain of command to the Administration Bureau Office for approval. The information shall include what computer applications need to be accessed and a copy of the applicable Memorandum of Understanding, if one exists.

   EXCEPTION: This does not apply to ALERT access; the individual would need to contact their agency's Terminal Agency Coordinator for access to ALERT.

2. When non-department personnel, no longer need access to KCPD computer systems, the responsible element will notify the Information Technology Division, so that access can be disconnected.

*G. Damaged or inoperable computer equipment:

1. Members will notify their immediate supervisor of any inoperable or damaged computer equipment.

2. If damage has occurred, supervisors will be responsible for reviewing the circumstances and determining whether the damage was incidental or negligent. Supervisors will contact Information Technology Division or Communications Support Unit.

ELECTRONIC MAIL (E-Mail) COMMUNICATIONS

*A. Use of the e-mail system by any member implies both understanding and compliance with this directive. Members using e-mail will do so in an appropriate and professional manner. Email that is distasteful, disruptive, offensive and unlawful will tarnish the professional image of the department.

*B. All messages generated on or handled by Microsoft Outlook, including back-up copies, are considered property of the department, not the member and are subject to Sunshine Law requests with the exception of those covered by Attorney/Client Privilege.

*C. Members will have no expectation of privacy in anything they store, send or receive on the e-mail system. The department may monitor e-mail without prior notice to the member.

D. E-mail has been implemented for official use only. Incidental personal use is permissible as long as it does not interfere with productivity or preempt official use.

*E. Members should refer to the support link on the intranet for information on how to setup Microsoft Outlook for the first time on their department computer.

F. Every department member is encouraged to use e-mail when appropriate. Appropriate uses include, but are not limited to:

1. Routine messages, announcements, notices, or other information that previously would have been disseminated via memorandum through the chain of command or by interdepartment mail.

*2. Any message currently being sent via facsimile, by voice over the telephone, or over a paging system.

EXCEPTION: Any ALERT, MULES, NCIC, NLETS or any other criminal justice data cannot be sent via e-mail outside the kcpd.org or leo.gov domain. Any questions regarding dissemination of this material should be directed to Alert@kcpd.org.

3. Drafts of reports, projects, or proposals.

4. Certain non-confidential department documents such as Job Vacancies, Department Memorandums, Bureau Memorandums, or Special Orders.

G. Unless approved by the Chief of Police or designee, e-mail will not be used for:

1. Disseminating confidential materials or department sensitive information, official documents that must be retained in their physical form, or documents that require a physical signature to certify receipt.

2. Non-department related charitable endeavors.

3. Private business activities.

4. Inappropriate entertainment purposes.

H. Members will check their e-mail inbox on a regular basis to ensure timely dissemination of information.

*I. Due to the nature of e-mail, any data sent over the department e-mail system is susceptible to purposed or inadvertent discovery.

INTERNET USAGE

A. Employees must use the Internet in accordance with all applicable laws and regulations. This includes compliance with copyright and license laws governing programs, as well as data and written materials accessed, obtained or provided to others via the Internet.

B. Members will not download software from the Internet without prior approval from Information Technology Division.

NOTE: To prevent inadvertent downloading, Internet users should be wary of pop up menus or advertisements that suggest doing so.

C. Prohibited uses of the Internet include but are not limited to the following:

1. Using Internet connections for private gain or profit, or to solicit for political, religious, or other non-business purposes.

2. Deliberate attempts to degrade or disrupt system performance may be considered criminal activity with possible prosecution under applicable state and federal laws.

*D. The following websites and site categories will be blocked from access:

1. Gaming Sites – Any website that facilitates or promotes gambling

2. Pornographic and Adult Content Sites

3. Hate Sites – Any site sponsored by militant or extremist groups that promote racism and hateful opposition to or action against segments of the population

4. Software Download and Installation – Downloading and installation of software from the Internet is a violation of current policies and procedures

5. Streaming Audio and Video

*E. As a business practice, accessing restricted websites or site categories may aid in combating crime and pursuing the criminal element. Therefore, any element or individual requesting access must establish a business case and forward the request through the chain of command. In consultation with the Information Services Division, exceptions may be granted. A business case is business related facts and circumstances that justify the need.

F. The use of the Internet is not a private matter and the department reserves the right to monitor all uses without notification to the member; audits will be conducted by the Information Technology Division, as required.