KANSAS CITY, KANSAS POLICE
GENERAL ORDER

ORDER NUMBER: **80.08**
ISSUED DATE: 10/17/2014
EFFECTIVE DATE: 10/24/2014
RESCINDS: 80.08, issued 03/16/2012

SUBJECT: Responsible Use of Information Technology

REFERENCE: CALEA LE Ch.41, 82; CO Ch 6; TR Ch 8

CROSS REFERENCE: 80.1

CONTENTS:

I. PURPOSE

A. To establish policy and procedure related to the use and security of computers, software, electronic messaging devices and the internet. It is the responsibility of Department members to use Information Technology in an efficient, ethical and lawful manner.

B. It is the policy of the Kansas City, Kansas Police Department that Information Technology resources provided to employees be used for the benefit of Department business and that they be used productively.

II. DEFINITIONS

A. Information Technology (IT**) –** includes but is not limited to the Department's computer network, servers, routers, switches, computers, pagers, landline telephones, wireless phones, PDA's, fax machines, printers, scanners, electronic mail, voice mail, mobile data computers and other devices

B. Computers – storage systems, servers, desktop, laptop and mobile computers to include the central processing units, monitors, printers and any other networked or non-networked peripheral devices.

C. Users – Employees that have been granted access to IT Resources.

D. Pagers – Department issued paging devices.

E. Telephones – Department landline based telephones as well as department issued wireless phones.

F. PDA – Department issued personal digital assistant (Palm Pilot, Handspring, IPaq, etc.).

G. Fax Machines – Department owned facsimile machines including copy machines capable of this function.

H. Electronic Mail – E-mail to include Department supported e-mail using Microsoft Outlook and an Exchange server as well as any other e-mail service that is capable of sending or receiving electronic mail to a Department owned computer or across the Department's network.

I. Social Media – Any forum on the World Wide Web on which people can share ideas or information. This includes, but is not limited to Facebook, Twitter, and LinkedIn, etc.

J. Instant Messaging – Software or service that allows real-time chatting between users.

K. Voice Mail – Messages recorded on an individual or unit telephones when a human operator is unavailable.

L. Mobile Data Computers – Mobile computers capable of accessing the Department's networks and/or criminal history information.

M. Systems Administrator – The person(s) designated by the Chief of Police to administer the Department's network.

N. KCJIS – Kansas Criminal Justice Information System, which allows access to criminal history and other law enforcement information through the Kansas Bureau of Investigations.

O. NCIC – National Crime Information Center, which allows access to criminal history and other law enforcement information through the Federal Bureau of Investigation.

III. POLICY

A. The Department provides components of sworn and civilian employees with Information Technology resources to more effectively accomplish the goals set forth by the Chief of Police. No other use of these devices is authorized.

B. All IT resources including all messages and data sent, received or stored on these resources are and remain the property of the Department. IT resources are not and should not be considered confidential or private.

C. The Police Department may monitor, audit, intercept, access, and disclose all data, recordings, or messages created, received, or sent using IT resources.

D. Password Procedures

1. Users are responsible for the security of their own passwords and Secure ID Tokens.

2. Sharing passwords and/or Secure ID Tokens is strictly prohibited and violates KCJIS and NCIC rules and regulations as well as this order.

3. Passwords must be changed routinely. This includes network logon as well as individual software logon passwords.

4. Users will be forced to change their passwords every forty-two (42) days if they do not do it more often on their own.

5. Passwords should contain letters and numbers, upper and lowercase characters for the greatest security.

6. Passwords should not be easily surmised. Users should avoid using names of family members, pets, significant dates or serial numbers as passwords.

7. Users cannot use the same password for at least five password changes.

8. Passwords will not be displayed on or around any IT resource where another user could potentially view it.

9. A Systems Administrator will remove any user whose employment ends, is terminated or suspended and will submit an annual report documenting the audit.

   a. A Systems Administrator shall perform a monthly inspection for access violations, improper use, and verification of all authorized users. A monthly and annual report (ref: G.O. 10.6, Appendix) verifying that the inspection has been properly conducted will be completed and forwarded to the Research and Development Unit. (In accordance with policy, passwords themselves are never directly accessed by the System Administrator. Password security is the responsibility of the user.).

10. A computer user, who has been authorized to use a password or protected account, may be subject to both criminal and civil liability, if the user discloses the password or makes the account available to unauthorized users without permission from the system administrator.

E. Copyright and licensing restrictions will be adhered to on all IT resources. Periodic checks of the contents of IT resources will be conducted routinely by the Systems Administrator to insure compliance. The Systems Administrator will remove any software found in non-compliance immediately upon discovery.

F. Fraudulent, harassing, threatening, discriminatory, sexually explicit, offensive/obscene messages or materials shall not be created, transmitted, printed, requested, or stored using any Department IT resource, except when necessary as part of an investigation.

G. Spam mail, viruses and computer hackers pose threats to Department IT resources. Users are not to open e-mail messages unless they are certain of the trustworthiness of the source. Messages received that likely contain inappropriate material will be deleted immediately. Messages received that appear suspect, e.g. unknown sender and/or a suspect subject, should be reported to the Systems Administrator prior to opening or viewing as it may contain a virus.

   1. Viruses and hackers pose a significant threat to all Departmental computers and IT resources. They can disrupt, disable, and crash the network system rendering files, cases and personal information unreadable, unusable and helpless.

   2. Hackers can infiltrate Department IT resources and compromise and steal confidential files.

H. Electronic messages (email) lists are intended to send information directly to that particular group. The user of the email list is responsible for determining the purpose of the list before sending messages to the list. Person(s) sending to a mailing list any materials which are not consistent with the list’s purpose will be viewed as having sent unsolicited material.

I. The transmission and dissemination of electronic messages (email) to superior or subordinate employees will be treated the same as official Departmental written correspondence. Such messages will not be transmitted or disseminated outside an employee's immediate chain of command, unless the employee's supervisor first grants approval for such action. The transmission and/or dissemination will adhere to the Department's unity of command concept, as stipulated in section VI, of General Order 1.3, Organization & Duties.

J. In general, the department’s electronic messaging systems shall not be used to transmit commercial, political or personal advertisements, solicitations or promotions without the approval of the Chief of Police or Assistant Chief of Police.

K. Although a user may have access to electronic information beyond the scope of General Order 80.1 Criminal Records Information, (e.g. Appraiser’s Office, Jail Management, etc.) they do not have permission to release this information. Requesting parties are to be directed to the record holder to see that proper dissemination occurs.

L. An authorized user of the IT Network shall not seek information from other areas of the Network or other sites connected to our network, which would be considered outside that person(s) job assignment or classification, unless authorized through that person(s) chain of command. This would include, but not limited to, data, digital or printed copies of information.

M. Usage — Computer users must respect the rights of other computer users. Most department systems provide mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person’s information are a violation of department policy and may violate applicable law. Authorized system administrators may access computer users' files at any time for maintenance purposes. System administrators will report suspected unlawful or improper activities to the proper authorities.

IV. PERSONALUSE OF IT RESOURCES

A. Users are not permitted to load, install, run software or visit Internet sites that facilitate peer-to-peer file and music sharing, gaming, gambling, Instant Messaging or chatting, or other unauthorized activity.

B. Users are not permitted to upload, or save to disk or other media, and remove data belonging to the Department without the express permission of the Chief of Police or his designee.

C. Users are not permitted to use encryption devices on Police Department IT without authorization.

D. Department personnel are prohibited from displaying scanned or reproduced Department images, logos, patches or badges on a personal web site or social media sites without the express permission of the Chief of Police or his designee.

E. Department personnel should refrain from posting any information about the department on their personal social media sites. For example: pictures from crime scenes, information about calls for service, and derogatory comments about Department personnel, etc.(See G.O. 80.11 Social Media Policy)

F. Employees are expected to confine their personal use of social media during the workday to their breaks and or lunches. Employees whose personal use of social media during the workday exceeds these limitations will be subject to discipline.

G. Incidental and occasional personal use of IT resources including web browsing, e-mail and paging may be permitted as long as it does not:

1. Have the potential to harm the Department, or involve illegal activities

2. Disrupt the conduct of Department business (e.g. due to volume or frequency)

3. Involve any business activity other than the business of the Department. This includes for-profit and non-profit personal ventures, religious, or political cause, or other non-job-related solicitations.

H. Telephones, Pagers, and Voicemail. Personnel that have been issued Department wireless phones, pagers, and those that have access to their own business telephone line, will leave an appropriate professional greeting as deemed by the Division/Unit Commander.

I. Department issued wireless phones and pagers will be placed on a setting that will alert personnel of an incoming call or page at all times or when on call.

1. Exceptions:

a. Officers appearing in court are authorized to shut these items off in conjunction with the judge's order/policy.

b. Officers conducting certain police operations that would jeopardize the officer's safety if the items were left on, are authorized to shut them off during that particular incident, but must turn them back on immediately afterwards.

J. Cell Phones, Blue Tooth, and hands free devices are not to be used on calls for service within public view, unless for official Department business.

1. Department employees will not text on a Department or personal cellular phone while operating a Department vehicle.

2. Department employees will not use their cell phones to take photographs or videos of crime scenes, suspects, or any other police actions they have become involved in. Any photographs, videos, and/or recordings an officer takes while on duty is considered evidence and is discoverable during any criminal or civil court proceedings.

K. Reporting Problems – Any defects, clerical errors or security issues found in a Network System must be reported to the system administrator so that steps can be taken to correct the issue.

L. Introducing, using or having another person introduce or use hardware or software that is designed to gain unauthorized access to any IT resource by password cracking, port scanning, keystroke recording or other method is strictly prohibited.

M. Introducing, using or having another person introduce or using hardware or software designed to corrupt or destroy IT resources or cause other harmful effects is strictly prohibited.

V. STORAGE

A. Due to space limitations and cost considerations, email messages on the public safety mail server older than 90 days will be automatically purged. Messages that are purged will not be recoverable. These messages will include messages held in the “inbox,” “sent items,” “deleted items,” and any user folder created within the mailbox containing mail messages. Users of email are authorized to individually archive and retain any email message longer than 90 days, but this will require manually transferring these email messages to a “personal folder” to allow for long term storage.

B. Due to space limitations, Mobile Data Computer transmission log files will be purged after 60 days unless a specific request to retain for a longer period is received for a particular record(s).

C. Nothing in paragraphs S and T is intended to prohibit longer retention of any email, document, recording, computer file, or other record.

D. Department Fileservers, Application Servers, Mail Servers, Web Servers and Domain Controllers will be backed up to disk daily. A REAL TIME Backup copy of critical data is stored off site at the Communications Center

E. Computer Aided Dispatch (CAD) information is maintained on a CAD server at the Communications Unit. There is also a backup CAD server at the Communications Unit in case of a failure of the first server. All CAD information is relayed over the network to the PDRMS server at Police Headquarters on a daily basis. This server is backed up to tape daily.

F. All data storage devices, including computer hard drives, and printer hard drives will be erased or destroyed prior to being placed in the trash. This includes KCJIS information or any document that may contain CHRI data.