POLICY 415
RESPONSIBLE USE OF INFORMATION TECHNOLOGY

PURPOSE

The purpose of this Policy is to establish the standards and guidelines related to the use and security of City information technology and communication systems – including but not limited to computers, telephones, e-mail, Internet, software, hardware, and messaging devices.

This Policy intends to encourage Leawood employees to use our technology to its fullest in manner that is ethical, efficient, lawful, and used productively for the benefit of the City and in furtherance of City business. This Policy intends to discourage and eliminate inappropriate use of our technology.

POLICY

This Policy shall apply to all employees, contractors, temporary workers, vendors, volunteers, and other others granted access to the City's information technology systems for City business purposes. Information technology means all communication and computing devices and systems including, but not limited to, computers, Internet connections, Intranets, networks, servers, routers, switches, pagers, cell phones, PDA's, facsimile machines, printers, scanners, electronic mail, voice mail, storage systems, other devices, electronic equipment in general, and any data stored or kept in any of the above.

Use of the City's information technology resources is provided solely upon terms established by the City. Use of these systems imposes an obligation on employees to understand and comply with this Policy and such other requirements that may apply. Access to City information technology resources is a privilege that may be revoked at any time.

Improper use of City information technology resources will result in discipline, up to and including termination of employment. Improper use includes any misuse as described in this Policy, any misuse that would result in violations of other City policies, as well as any harassing, offensive, demeaning, insulting, defaming, intimidating, fraudulent, threatening, discriminatory, obscene, or sexually suggestive written, recorded, or electronically retrieved or transmitted communications.

The Director of Information Services or his/her designated representative may, when necessary for City business; supersede Policy 415, "Responsible Use of Technology Information" and its related Procedures.

PROCEDURE 415-1
RESPONSIBLE USE OF INFORMATION TECHNOLOGY

OVERVIEW

This Procedure identifies the proper uses of information technology resources and communication systems.

STANDARD

The City hereby notifies all employees and management personnel that no member of personnel should have any expectation that their use of the City's technology is in any way private. The technology belongs to and is managed by the City and the City may access the technology when required and when the law permits.

Users should have no expectation to privacy in their use of the City's computer, telephone, and other technology systems, including any incidental personal use. The City may monitor, audit, intercept, access, and disclose all data and messages created, received, or sent using information technology resources. Passwords or access codes provided to any user to access the City's systems are granted solely for the purpose of ensuring and maintaining the security of the system and do not provide or create any personal right or expectation of privacy for any user.

General Computing & Network Systems

Use of the City's information technology systems reflects upon the professional image and public trust of the City government. Accordingly, use of the City's information technology resources shall be conducted in a responsible, professional manner.

Appropriate use of technology is essential to serving our internal and external customers, and employees shall:

- Ensure that outgoing messages, whether by mail, facsimile, e-mail, Internet transmission, or any other means, should be accurate, appropriate, and ordinarily be work-related.

- Use care in communicating confidential information and should take reasonable steps to ensure that the communication is properly identified and directed.

- Comply with the required or appropriate levels of confidentiality related to governmental information systems and records, including but not limited to that level of confidentiality required for the protection of Protected Health Information by HIPAA. Each user is responsible for the content of all text, audio or images that they transmit or store.

- Comply with all state, federal and contractual requirements and obligations related to the access and use of criminal justice information systems, including without limitation KCJIS, NCIC, and ALERT. Department directors are responsible for ensuring compliance with the requirements and limitations related to the use of criminal justice information systems and shall develop department-specific protocols for their use, where appropriate.

- Promote efficient use of the networks to minimize, and avoid if possible, congestion of the networks and interference with the work of other users of the network.

- When authorized, Transmit proprietary information only via secure communication systems.

- Employees may use the City's information technology resources for incidental personal use as long as it: 1) is brief and occasional; 2) does not interfere with the employee's work, another's work, or City operations; 3) does not violate any City policies, procedures, or rules; 4) does not violate the legal or contractual obligations related to use of the system. In no event shall criminal justice information systems be used for personal use.

The following use of technology is prohibited and individuals engaged in it will be subject to discipline, up to and including termination of employment:

- Sending personal correspondence that appears to be an official communication of the City

- Using City resources for personal gain or to conduct personal business.

- Sending threatening, harassing, slanderous, defaming, obscene or suggestive messages and images, political endorsements, commercial activities, or material that is discriminatory with regard to race, sex, religion, ethnicity, disability, and age are prohibited.

- Viewing, storing, displaying or transmitting any messages or images that contain defamatory, false or fraudulent, abusive, obscene, pornographic, profane, sexually-oriented, threatening, racially offensive or otherwise biased, discriminatory or harassing material is prohibited.

- Unnecessarily encrypting communications. Encryption devices and software including "bit locker" hard drive encryption technology must be approved by Information Services. prior to use

- Using "bios" / system passwords unless approved by the Director of Information Services or his / her designated representative.

- Disrupting or damaging any components of the City's information systems. Intentional attempts to "crash" the network or computer systems or programs are prohibited.

- Deleting, examining, copying, or modifying files and / or data belonging to other users without their prior consent.

- Accessing or attempting to gain unauthorized access to data, system resources, passwords, etc. or decrypting of system or user passwords.

- Copying or deleting of network system, operating system, and application software.

- Attempting to secure a higher than assigned level of privilege as assigned by Information Services on the network or on specific technologies.

- Loading of any software or installing hardware on the City's computers or network systems unless approved by Information Services.

- Playing of any computer games at any time.

- Intentionally introducing computer "viruses" or other disruptive programs into the City's systems. Introducing, using, or accessing software or hardware devices designed to corrupt or destroy information technology resources or cause any harmful effect.

- Sharing your passwords with others unless approved by your Department Head and Director of Information Services.

Electronic, Voice, & Text Messaging

Electronic messaging, in general, lends itself to a more relaxed and less guarded way of communicating which could lead to misunderstandings and unwarranted liability. Communications that would be inappropriate under other City policies are equally inappropriate in e-mail, voice-mail, or text messages.

Electronic messaging is City equipment and hence all material is City property. Information thought to be "erased" or "deleted" remains on back up storage devices for extended periods of time.

Following are examples of appropriate use of electronic, voice, and text messaging. The list is not all inclusive.

- Manage e-mail and voice-mail inboxes and associated folders. Messages that require long-term retention should be stored in specific folders or printed, if necessary.

- Contact Information Services before attempting to install any attachments with file extensions including but not limited to the following: exe, bat, vbs, com, msi,or other type of "installation/executable" program files.

- Open e-mail attachments and links only if you are expecting them from a known source and feel confident they don't contain viruses, malware, or other unwanted material or programs. E-mail attachments or links may host viruses or may be attempts at gathering personal and City identification information. Otherwise known as "Phishing" e-mails, these e-mails are very misleading and attempt to trick you into providing confidential and personal identification information. Delete these and other "suspicious" e-mails immediately.

- Use appropriate language. Don’t put anything in e-mail that you would not broadcast to the general public.

Following are examples of inappropriate use of electronic, voice, and text messaging. The list is not all inclusive.

- Sending junk mail or “chain” letters.
- Falsifying or appropriating another user’s identification or accessing another user’s voice-mail or e-mail account without his/her express consent.
- Sending or exchanging pornographic e-mails or messages in any format.
- Interfering with City operated and installed anti-virus and/or anti-spyware software. Employees are expected to follow all instructions for cautious use.
- Exchanging messages likely to result in the disruption or loss of the recipient’s work and/or other uses that are likely to cause congestion of the network or telephone systems, or otherwise interfere with work.

Internet Access & Usage

Internet technology allows employees to more efficiently provide service and must be used appropriately.

- Internet access is granted to employees as a tool to do City business. Reasonable personal access is allowed during non-work hours subject to department or supervisor's restrictions. There should be no expectation that any use of the City's technology systems are in any way private.
- Be aware that file downloading and uploading from and to the Internet creates significant network traffic which can consume City bandwidth.
- Employees are required to adhere to all applicable licensing and intellectual property restrictions. Employees should not duplicate, introduce or download from the Internet or from an e-mail any software or materials that are copyrighted, patented, trademarked, or otherwise identified as intellectual property without express permission from the owner of the material. .
- Periodic checks of the contents of technology resources may be conducted to ensure appropriate use and licensing.
- Accessing adult entertainment, pornography, suggestive or any other inappropriate material, at any time from any City facility or vehicle is prohibited regardless of whether or not you are using City or personal equipment.

- Using City equipment at any time or place to access adult entertainment, pornography, suggestive or any other inappropriate material is prohibited.

Data Protection & Confidentiality
The City will only collect personal information for employees and others if it is required to pursue its business operations and to comply with government reporting and disclosure requirements. Personal information collected by the City includes employee names, addresses, telephone numbers, email addresses, emergency contact information, EEO data, social security numbers, driver's license numbers, date of birth, employment eligibility data, benefits plan enrollment information, which may include dependent personal information, and school/college or certification credentials, credit card information, bank accounts, and other similar information. All pre-employment inquiry information and reference checking records conducted on employees and former employee files are maintained in locked, segregated areas.

If an employee becomes aware of a material breach in maintaining the confidentiality of any confidential information, the employee should report the incident to the Director of Human Resources or a representative of the Department of Human Resources.

- Personal information will be considered confidential and as such will be shared only as required and with those who have a need to have access to such information. All hard copy records will be maintained in locked, secure areas with access limited to those who have a need for such access. Personal employee information used in the Human Resources and Payroll Information System (EDEN) applications will be safeguarded under proprietary electronic transmission and intranet policies and security systems

- City-assigned information, which may include organizational charts, department titles and staff charts, telephone directories, e-mail lists, facility or location information and addresses, is considered by the City to be proprietary information to be used for internal purposes only. The City maintains the right to communicate and distribute such information as it deems necessary to conduct business operations.

- The Department of Human Resources will investigate, or refer to the appropriate department, all incidents of alleged material breaches of confidentiality in order that appropriate corrective action may be taken.

Examples of the release of personal employee information that will not be considered a breach include the following:

- Partial employee birth dates, i.e., day and month may be shared with department heads that elect to recognize employees on such dates.

- Personal telephone numbers or e-mail addresses may be distributed to department heads in order to facilitate work schedules or business operations.

- Employee identifier information used in salary or budget planning, review processes and for timekeeping purposes may be shared with department heads.

- Employee’s employment anniversary or service recognition information may be distributed to department heads periodically

- Employee and dependent information may be distributed in accordance with open enrollment processes for periodic benefit plan changes or periodic benefits statement updates.

- Employee and dependent personal information may be shared with plan providers as required for claims handling or record keeping needs.

- All information available under the Kansas Open Records Act.