Rule 3-35

USE OF INFORMATION TECHNOLOGY

§§:

§ 3-35-010 PURPOSE

The purpose of this rule is to ensure that the use of information technology in the work place is consistent with federal and state laws and county policies and rules for public records, ethics, and conduct of employees.

§ 3-35-020 APPLICABILITY

These rules apply to all forms of information technology, hereafter referred to as "systems," including but not limited to electronic systems such as email, fax, voice mail, internet, computers, software, networks, cellular devices, smartphones, tablets, digital assistants, pagers, and electronic publishers. Personal systems used for work purposes and county owned systems provided for use from home or other locations are subject to this rule. Systems owned and operated by third parties having a business relationship with the county who store or process county information for county business purposes are subject to this rule.

§ 3-35-025 DEFINITIONS

ACCESS: Rights an employee has to read or write electronic data, log in to county owned or authorized systems, files, networks or execute applications using county owned or authorized systems. For example, a user might be granted read access to a file, meaning that the user can read the file, but cannot modify or delete it. Most systems have several different types of access privileges that can be granted or denied to specific users or groups of users. This definition also includes rights an employee has to read, copy, retrieve, or otherwise make use of non-electronic data, information and/or files of any kind.

COUNTY AUTHORIZATION: Authorized by the county's Chief Information Officer, one or more elected officials, or individuals delegated such authority by aforementioned persons under county procedures implementing this rule, and/or MCPR 3-36 Social Media Policy and/or 3-37 Cellular Devices.

CUSTODIAN OF RECORDS: The county official or employee who is responsible for keeping the public record on file.

DEPARTMENT AUTHORIZATION: Authorized by the Department Director or designee.

DISCLOSE: To in any way, make known, reveal, or allow information to be seen by another county employee or member of the public.

ELECTRONIC PUBLISHING: The activity of making information available for public view.

ELECTRONIC RECORDS: Records which are stored in a form that require a computer or other electronic device to process.

INFORMATION TECHNOLOGY: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

MIXED USE: Use that is not required for the job, but relates to county employment and/or enhances the ability to perform job duties.

PUBLIC RECORD: Documents, books, papers, photographs, files, sound recordings, or machine readable electronic records, regardless of physical form or characteristics, made, received, filed, or recorded pursuant to law or in connection with the transaction of public business, whether or not confidential or restricted in use. Public records do not include extra copies of a record, preserved only for convenience of reference, or messages on voice mail or other telephone message storage and retrieval systems.

§ 3-35-030 POLICY

(A) The county encourages the use of electronic systems, communications, and information technology to support the mission and business of the county. All systems and information are the property of the county, except for personal cellular devices used for work purposes as provided in MCPR 3-37 and this rule. Employees may use systems only for authorized county business except as otherwise provided for in this rule and MCPR 3-37. Systems use must be inoffensive, in accordance with all federal and state laws, county rules, regulations and procedures established by county departments and work units, and reflect a positive county image. Social media usage is a use of information technology. As such, use of social media during work hours or using county systems including county-issued cellular devices and personal cellular devices approved for utilization for work purposes must comply with MCPR 3-36 Social Media Policy, MCPR 3-30 Code of Ethics, MCPR 3-37 Cellular Devices, and this rule.

(B) County employees are permitted brief and infrequent personal use of county systems if the use does not interfere with official business, is at virtually no cost to the county and is in accordance with state ethics laws and rules. This limited personal use must take place during the employee's non-work time and is considered an incidental benefit under MCPR 4-20-110.

§ 3-35-040 ACCESS AND CONTROL

(A) County Access and Control

(1) No part of county systems or information may become the private property of any system user. The county reserves all legal rights to full access and ownership of its systems, to transfer, or to use all or any part or product thereof, and to all information used in its systems. All uses must comply with this rule and all other laws, rules, regulations, and procedures.

(2) Information technology and electronic communications will be used only for county business, except as otherwise provided in these rules. No one will grant access to systems without county management authorization.

(3) All software loaded on county systems must comply with software licensing requirements and be approved by the county Information Technology (IT) Department.

(B) Employee Systems Access

(1) Employees only have the right to access systems and information for authorized purposes and in an authorized manner, and in accordance with any relevant laws or policies. Accessing county systems or information in non-authorized ways is prohibited. Employees are allowed to gain access to another employee's electronic mail, voice mail or other system files only as allowed by § 3-35-050(B)(4) or with permission from a supervisor, and only if such access is not prohibited by law or other policies.

(2) Employees may not load privately owned, free, or shareware software on county systems or devices, nor connect (i.e. hard wire, wireless connection or by any other means) any privately owned device to a county system without county authorization, regardless of purpose.

(3) Employees will not disclose or share passwords unless authorized to do so by their supervisors as required for system maintenance or other authorized purpose and not prohibited elsewhere in these rules. When the limited circumstance or event concludes, employees will update the shared password to one that only they know. Employees with administrative passwords will only use these passwords for authorized purposes and in an authorized manner.

(4) Employees will not view, use, disclose or alter data in a county system for other than business purposes or unless county authorization is received first. In all cases, system event log data (including security and other operational logs) may not be altered once written to the log.

(C) Limiting or Revoking Access

The county may revoke or limit permission for use of county systems for any or all personal or business uses at any time without cause or explanation. Department Directors may issue department specific limitations on personal use that are more restrictive than this rule.

(D) Confidentiality of Systems and Information

(1) Various county, state and federal laws, rules, regulations and policies restrict access to and disclosure of confidential and sensitive data and information, such as employee or client medical information, financial information, social security numbers, etc. Employees will not disclose or allow access to such sensitive and confidential information or data, except in accordance with county or departmental rules, practices or procedures. Employees with such access are responsible for the safekeeping and handling of electronic systems to prevent unauthorized disclosure of financial, medical, and other personal client or employee information, or any other confidential information contained in the system.

(2) Electronic data should be transported only as needed to conduct county business. Employees are required to ensure that data transported within or outside of county facilities on laptops, CDs, or other storage devices are properly secured.

§ 3-35-045 EMPLOYEE PRIVACY EXPECTATIONS

(A) County employees do not have a right, nor should they have an expectation of privacy or confidentiality while using county systems, including but not limited to, electronic or voice mail or use of social media. County employees do not have a right, nor should they have an expectation of privacy or confidentiality in work records on their personal cellular devices used for work purposes whether or not the employee is compensated for its use per MCPR 3-37. Employees are expected to provide to the County work records on personal systems used for work purposes, to the extent required by public records laws and other legal requirements.

(B) The county may trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information on county-owned systems or work records located on personal devices used for work purposes, at any time without notice unless prohibited by law. The county has the right to access, monitor and record all electronic and voice mail or other county-owned systems at any time and without notice unless prohibited by law. The county will only monitor or record telephone calls as permitted by federal and state law. The county may use this information in disciplinary or other legal proceedings.

§ 3-35-050 ACCEPTABLE USE

(A) Standards for Electronic Communications or Systems Access

(1) Uses of county systems and personal cellular devices for work purposes do not always have to be formal, but the usage must positively reflect the image of the county.

(2) All uses must be lawful and inoffensive. Uses of county systems and personal cellular devices for work purposes must not be false, unlawful, offensive, or disruptive. Unless county duty requires it, no use will contain profanity, vulgarity, sexual content, or character slurs. No use will make rude or hostile reference to race, color, sex, age, religion, national origin, political affiliation, marital status, sexual orientation, gender identity, source of income, familial status, or physical or mental disability, or otherwise violate county policy or law. Use will not include gambling or other

potentially illegal activity. All uses must comply with federal, state and county laws and regulations, and other county policies.

(3) Copyrighted or licensed information of any kind will be used only with full legal right to do so. For example, this rule requires that the county or individuals using commercial software must honor the licensing agreements that govern the use of that software.

(B) Internet and E-mail Use

(1) Employees may access or download information from internet sites for official business subject to county or other departmental procedures.

(2) Employees may not download software, shareware, or music from the internet without county authorization.

(3) Many internet and e-mail groups exist to share useful information. An employee may post job-related queries or comments to professional group message boards, listservs or emails with supervisory authorization. Comments must conform to this policy. Content and frequency of posting must reflect county interests, not the users'.

(4) Department Human Resources Units, Central Human Resources, and the County Attorney's Office may request reports detailing employee usage of county-owned cellular devices, and internet and email usage on county-owned systems. These reports include information that specifies internet sites employees accessed or attempted to access, how long employees spent on internet sites, and copies of emails or similar messages sent and received. Managers who believe they need access to usage reports shall contact their Department Human Resources Unit for approval to access such reports.

(5) When posting on the internet for non-work purposes, employees may not use their county job title, email address or other information showing county affiliation in a way that indicates they are acting as county employees.

(C) Publishing Electronically

(1) All publishing is restricted to county business as defined by departments and requires department authorization, including posting using social media, unless allowed in other sections of this rule.

(2) Department- or county-wide e-mail messages require department or county authorization. Events which mix county and personal business, such as charitable drives, employee retirements, celebrations, or whatever the department deems suitably related to department business may be published with department authorization.

(D) Personal Use of County Systems

Any personal use must comply with all personnel rules and must be consistent with the following:

(1) Personal use of county systems, including information technology tools, must always be at virtually no cost to the county, and brief and infrequent. In addition to uses which have a direct cost, such as making toll calls, personal uses which have an indirect cost are also prohibited, including but not limited to uses which require significant data storage or data transmission (bandwidth) capacity. Examples include, but are not limited to, sending or receiving personal emails with large file attachments, personal emails which contain graphics, photos, or sound files, and storing large files of any kind on shared servers or local drives.

(2) Personal use must be brief and infrequent in terms of time used as compared to use for assigned work and may only be done during breaks and non-work hours. Accessing personal emails through internet providers such as AOL, Yahoo or Google, must be done in such a way as to ensure county systems are not compromised by viruses or other threats. Employees should not open emails using the county systems unless the sender is known to them. More specific rules for the use of cellular devices are included in MCPR 3-37 Cellular Devices.

(3) Permissible personal uses include:

(a) A brief e-mail message.

(b) A pager message.

(c) A short toll-free fax.

(d) Copying or printing a small number of personal papers, provided the use of equipment is brief and infrequent, and does not interfere with county business.

(e) Brief and infrequent use of a personal computer.

(f) Brief and infrequent web searches for personal research, or self-study.

(g) Brief and infrequent postings using social media if the content or purpose is personal.

(h) A brief and infrequent telephone call.

(i) A brief and infrequent toll call that is not charged to the county.

(j) Brief and infrequent storage of copies of personal electronic files (no more than 500 megabytes) e.g., photographs of family members or friends as long as they have been virus scanned.

(k) If the employee is not assigned a county desk phone the employee may use a county-issued cellular device in the same manner as a desk phone so long as it amounts to virtually no cost to the county, or if it results in additional cost for the county, the employee will reimburse the county for the added cost.

(l) Data streaming on a county-owned computer or cellular device provided there is no interference with county business including impacts on county data storage or transmission (bandwidth) capacity. For county-owned cellular devices, a WiFi connection must be used for data streaming, and not the county's cellular data plan.

(m) Downloading a third-party application or "app" on a county-owned cellular device provided there is no cost or charge to the county and no interference with county business.

(4) Mixed use

Permissible mixed county and personal uses include downloading, printing and photo copying a county job application, personnel and benefits papers, and necessary material for county paid courses of study, so long as such usage is brief and infrequent.

(5) Prohibited personal uses include but are not limited to:

(a) Except as provided above in § 3-35-050(D)(3) and in MCPR 3-37, toll calls, any service for fee, and downloading software or shareware.

(b) Personal soliciting.

(c) Lobbying, soliciting, recruiting, selling, or persuading for or against commercial ventures, products, religious or political causes, outside organizations, or similar activities.

(d) Using county systems or allowing others to use them on behalf of any organization or third party.

(e) Internet games, personal games, and internet gambling sites may not be used or accessed except as authorized for work purposes. Games that come with software may be used only with department authorization for work purposes. The games will be used without sound and only where not visible to the public. County owned or licensed games created to teach needed knowledge or skill may be used with department authorization for work purposes.

(f) An employee may not use for personal business any system device that the employee does not use in his or her assigned work.

(g) No privately owned device may be physically connected (hardwired or wireless) to county systems without county authorization. System devices taken home or for use off county premises remain subject to this policy.

§ 3-35-055 SANCTIONS

Employees who engage in improper use of information technology and electronic communications under this rule are subject to disciplinary action, up to and including dismissal.

§ 3-35-060 ELECTRONIC RECORDS RETENTION AND ACCESS

(A) Electronic records stored on county information systems are public records. As such, the records are subject to the same laws and rules for public inspection and retention that apply to all other county records, including but not limited to the state public records laws and rules, county Executive Rule 266 and county Administrative Procedure REC-1. Employees should refer to the retention schedules for their Department to determine what must be retained and what can be destroyed. Retention schedules are available at http://web.multco.us/records/retention-schedules.

(B) Electronic records may not be destroyed without proper authorization.

(C) Upon receipt of a valid request, the custodian of electronic records must make the records available for inspection by the public and copying unless the records are exempt from disclosure.

(D) Requests by the public for copies of or to inspect electronic records must be reviewed by the County Attorney's Office before providing copies or permitting or denying such inspection.

(E) The county may collect reasonable fees for making electronic records available for inspection or copying. Departments/Custodians may establish rules for access to records in order to protect the integrity of the records or to prevent interference with county business. Departments are encouraged to post fee schedules and access rules.

(F) Whether a public record is exempt from public disclosure shall be determined by the application of state law to the record based on its nature and content, regardless of the form in which the record is preserved.

(G) Employees must follow any county procedures for retention and management of electronic county records stored on non-county owned information systems or cellular devices.