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 workplace is consistent with information security best practices, federal and state laws, and county policies and rules for public records, ethics, and conduct of employees. Volunteers and interns (paid or unpaid) are also covered by this policy.

§ 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, voicemail, internet, computers, software, networks, mobile devices, smartphones, tablets, and internet subscription or cloud-based services. 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.

- **Authorized Approver**: An individual identified at the department level who has the ability to approve access to IT systems for their department.

- **Cloud-based Services:** Any service or internet subscription made available to users on demand that is hosted on a cloud-computing provider's infrastructure as opposed to being provided by the Multnomah County's own on-premise infrastructure.
- **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 MCPR § 3-37 Mobile Devices.
- **Custodian of Records:** The county official or employee who is responsible for collecting and maintaining records whose retention is required under Oregon law.
- **Department of Authorization:** Authorization 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 review.
- **Electronic Records:** Data or information that has been captured and fixed for storage and manipulation in an automated system and requires the use of that system to render it intelligible by a person.
- **Information Technology (IT):** 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.
- **Personally Identifiable Information (PII):** Any information about an individual maintained by Multnomah County, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. This includes all information protected by local, state and federal laws and regulations. For specific examples, see Multnomah County Administrative Procedure PII-O Personally Identifiable Information Definitions.
- **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 voicemail or other telephone message storage and retrieval systems.

- **Service:** The application of business and technical expertise to enable organizations in the creation, management and optimization of or access to information and business processes. A system which may include software, cloud-based services (such as Software as a Service (SaaS)), and the associated systems that provide a means to access data.

- **System:** A set of components for collecting, creating, storing, processing, and distributing information, including but not limited to electronic systems, such as email, fax, voicemail, internet, computers, software, networks, mobile devices, smartphones, tablets, and internet subscription or cloud-based services.

- **Software:** A generic term used to describe computer programs; a set of instructions or programs instructing a computer to do specific tasks, sometimes known as Scripts or applications. May also take the form of Software as a Service (SaaS), which is software that is not installed on a local device but accessed through the internet (see cloud-based service).

§ 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 devices used for work purposes as provided in MCPR § 3-37 Mobile Devices and this rule. Employees may use county-owned systems only for authorized county business except as otherwise provided for in this rule and MCPR § 3-37 Mobile Devices. 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 Mobile 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 Benefits: Incidental Benefits.

C. County-owned IT devices may be taken home or to other locations for work purposes by employees with prior approval of their manager. All equipment shall be returned upon separation from employment with the County.

§ 3-35-040 Access and Control

A. County Owned Devices

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, including to transfer or 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 be granted access to data, systems or services without written authorization by a Multnomah County Authorized Approver. Authorized Approvers may not authorize their own access to data, systems or services.

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

4. A user is not allowed to download or install any software or accept the terms of any software or cloud service agreement including “click through” agreements unless given written authorization from County IT (or DCA Procurement and Contracting). These agreements include but are not limited to: End User License (EULA), Software / Cloud Service Agreements or Terms of Use / Service.

5. All internet subscription and cloud based services must comply with licensing requirements and be approved by the county Information Technology (IT) Division.

6. When in a Multnomah County facility, personal devices may only connect to the Multco Guest County Wi-Fi network.

B. County Systems Access

1. Employees only have the right to access county 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, voicemail or other system files only as allowed by MCPR § 3-35-050(B)(4) or with permission from a manager, 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. wired, wireless connection or by any other means) any privately owned device to a county system without county authorization, regardless of purpose.

3. Under no circumstance should an employee share their personal passwords. unless authorized to do so by their supervisors as required for an emergency. Passwords should never be written down or in an unsecured manner. Employees with administrative passwords or accounts will only use these passwords for authorized purposes and in an authorized manner. A shared system password may only be used with written permission by the County Security Officer.

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 personally identifiable information. 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 county systems to prevent unauthorized disclosure of financial, medical, and other personal client or employee information, or any other confidential information contained in a system.

2. Electronic data should be transported only as needed to conduct county business. All personally identifiable information that must be transported or otherwise sent outside of county facilities must be encrypted with county provided encryption technology or other county authorized mechanism. Employees are required to ensure that data transported within or outside of county facilities on laptops, 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 voicemail or use of social media. County employees do not have a right, nor should they have an expectation of privacy or confidentiality regarding 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 Mobile Devices.

B. The county may trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information on county-owned systems at any time without notice unless prohibited by law. The county has the right to access, monitor and record all electronic and voicemail 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.

C. Upon request, employees will provide to the County any work records on personal devices and third party websites used for work purposes, including but not limited to emails, electronic documents, texts, chats, voicemails, and social media posts, whether or not the employee is compensated for its use per MCPR § 3-37 Mobile Devices, to the extent required by public records laws and other legal requirements. The county may use this information in disciplinary or other legal proceedings.

§ 3-35-050 Acceptable Use

A. General Standards for Electronic Communications or Systems Access

1. Uses of county systems and personal mobile 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 mobile 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 and all employees using commercial software on its behalf must honor the licensing agreements that govern the use of that software.

B. Internet and Email 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 from the County Information Technology (IT) Division.

3. Many internet and email groups exist to share useful information. An employee may post job-related queries or comments to professional group message boards, listservs or emails with manager authorization. Comments must conform to this rule. 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 mobile 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, and how and when employees accessed County-owned facilities. Managers who believe they need access to usage reports shall contact their Department Human Resources Unit for approval to access such reports.

5. The county prohibits the global (automatic) forwarding of email to an email account not managed by Multnomah County unless explicitly authorized by the County Security Officer. Protected health information may never be forwarded to an employee's personal email account.

6. Sending or selectively forwarding email that contains Protected Health Information (PHI) is only allowed if the employee first verifies the identity and authority of the recipient, the disclosure of protected health information is a part of an approved workflow, and the email is encrypted using county provided encryption technology.

7. When posting on social media 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

E. 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 mobile devices are included in MCPR § 3-37 Mobile Devices.

3. Permissible personal uses include:

    a. A brief e-mail;

    b. A brief text 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, e.g., photographs, documents, and digital music, so long as they have been virus scanned with any software the County has made available for that purpose;

k. If the employee is not assigned a county desk phone the employee may use a county-issued mobile 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; and

l. Data streaming on a county-owned computer or mobile 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 Wi-Fi connection must be used for data streaming, and not the county's mobile data plan.

4. Mixed use: Permissible mixed county and personal uses of county systems include downloading, printing and photocopying 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 MCPR § 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 a county issued device for the purpose of operating a personal business; and

   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 rule.

§ 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 Multnomah 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 on the Records Management website.

B. Electronic records may not be destroyed without proper authorization, either via a retention schedule published on the Multnomah County Records Management website or through direct consultation with a records management analyst. See Multnomah County Administrative Procedure REC-1.

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. See Multnomah County Administrative Procedure REC-2.

D. Requests by the public for copies of or to inspect electronic records must comply with Multnomah County Administrative Procedure REC-2, including review by the County Attorney's Office (as applicable), and any Department or Division policies.

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 County Attorney's Office based on its nature and content, regardless of the form in which the record is preserved.

G. Employees must follow all county procedures for retention and management of electronic county records stored on non-county owned information systems or mobile devices. Records in non-county owned systems with retention periods of five years or longer must have a preservation plan approved by a records management analyst in order to reduce risk of loss or obsolescence during the full retention period, and for portability to a new information system or for duplication in response to a public records request.