

Jefferson County

Employee Administrative Rules & Regulations

Use of Phone, Email, Computer and Information Systems



Rule Number: 5.1.25
Date Established: Administrative Order #04-1 – 4/27/04
Administrative Order #89-2 – 9/12/89
Date of Last Revision: 4/1/2018
Date of Current Revision:

1.0 PURPOSE

The purpose of this Rule is to establish a rule for the use and security of Jefferson County Commission's computers¹ and email system.

2.0 RULE

The County's computers, phones and email systems are for the exclusive use of Jefferson County employees. Data housed on the County's computers may only be accessed by County employees for the purpose of conducting County business. All technology provided by the County, including computer systems, communications networks, company-related work records and other information stored electronically, are the property of the company and not the employee. Occasional use of County email for personal communication is not inherently a violation of this Rule. However, such use may be restricted or terminated by a supervisor for abuse.

All County employees must sign and have on file a Computer and Email Usage Rule Acknowledgment Form (Figure 1) before being granted access to any County computer.

All data created, received and sent by employees using County systems, whether for business or personal use, is the County's property and is subject to monitoring. Employees should not have any expectation of privacy in data created on or transmitted through company systems, including personal email accounts. Internal and external e-mail, voice mail, and text messages are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the company. The County reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite.

¹ The term "computer" as used throughout this Rule includes any and all electronic devices issued by the County.

Every employee of the County is responsible for the content of all text, audio or image files that he or she places or sends over the organization's Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. The County's identity must be attached to all outgoing e-mail communications and they should reflect our values as well as appropriate workplace language and conduct

Non-public, proprietary, or otherwise confidential data housed on County computers or databases may not be released to any member of the public or to any party external to the County without proper authorization.

Electronic forms, templates, databases, reports, and other documents used in the course of business may not be secured or protected with a personal User ID and/or password. If there is a need to restrict access to such material, a user ID and password shall be established and used for this purpose and must be known by no less than the originator of the password and the supervisor of the department responsible for the file.

With the exception of IT staff providing support or assistance, no County employee may give or use his or her own password, security badge, or credentials to obtain access for another employee without express authorization from a supervisor to do so. No employee may use any other employee's password, security badge, or credentials.

No County employee may perform any unauthorized or illegal transaction with a County computer, regardless of security access. In addition, employees are prohibited from using for any purpose without proper authority any County computer that is not assigned to that user. To prevent contamination of the County's technology and communications equipment and systems by harmful computer viruses, downloaded files are automatically checked for possible infection by the IT department. Also, given that many browser add-on packages (called "plug-ins") may not be compatible with other programs and may cause problems for the systems, downloading plug-ins is prohibited without prior permission from IT.

Employees may not use the County's Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted. Harassment of any kind is prohibited.

Disparaging, abusive, profane or offensive language; materials that might adversely or negatively reflect on the County or be contrary to its legitimate interests; and any illegal activities—including piracy, cracking, extortion, blackmail, and unauthorized access to any computers on the Internet or e-mail—are forbidden.

Copyrighted materials belonging to entities other than the County may not be transmitted by employees on the network without permission of the copyright holder. Employees must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy for reference only. Saving copyright-protected information to a network drive without permission is prohibited. Sharing the URL (uniform resource locator or "address") of an Internet site with other interested persons for business reasons is permitted.

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to IT, with the approval of the department head. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

It is the responsibility of County employees to:

- Adequately secure the computer(s) they use by locking and password protecting it when not in use.
- Adequately secure any personal device or computer used to remotely access County data or systems.
- Immediately report a lost, stolen, or damaged computer or other electronic device to his or her supervisor.
- Immediately report any actual or suspected data breach.

It is the responsibility of supervisors to contact the County's IT Department as soon as an employee resigns, is terminated, receives a disciplinary suspension, or otherwise leaves the employ of the County. All security rights to any County computer will be terminated immediately as of the date of separation.

It is the responsibility of each County Official and Department Head to provide publication and instruction to all of their subordinates of this Rule.

3.0 CONSEQUENCE OF RULE VIOLATIONS

Violation of this Rule will subject an employee to formal disciplinary action, up to and including termination for the first offense.

Figure 1: Use of Phone, Email, Computer and Information Systems Rule

Use of Phone, Email, Computer and Information Systems Rule Acknowledgement Form	
<p>I hereby acknowledge that I have received a copy of Jefferson County Commission's Use of Phone, Email, Computer and Information Systems Rule. I understand that my use of the County's email and internet system constitutes my consent to all the terms and conditions of the Rule. I understand that the email system and all information transmitted by, received or stored in the system are the property of the County and is only to be used for business purposes.</p>	
<p>I further acknowledge that I have no expectation of privacy in the connection with the use of the internet and email system or with the transmission, receipt or storage of information in that system. I consent to the County's monitoring of my use of the email and internet, including the printing and reading all emails and data entering, leaving or stored in the system.</p>	
Employee Name: _____	
Employee Signature: _____	Date: _____
Supervisor Signature: _____	Date: _____