

CHAPTER I (GENERAL)

PR 106 Internet, E-Mail Usage & Social Media

A. Purpose

To establish a policy for employee use of Information Technology Systems (ITS), here defined as internal and internet e-mail, social media, internet, software programs, hardware, communication devices and general computer usage by employees of Yuma County. The County uses these sources to support and facilitate ITS delivery of County services. Inappropriate use of ITS IT systems could give rise to legal actions against the County and/or individual employees. Therefore, this policy applies to all County IT systems regardless of location (i.e., office, home, field locations, etc.) And any or all electronic devices used in County business or to access County IT systems. Each County employee who is or becomes an authorized user of the County's IT systems is required to sign the "acceptable use policy acknowledgement."

B. Policy

All IT systems owned or implemented by the County, and all content including but not limited to: messages, text, graphics, images, electronic files and other information transmitted by, received through or stored in these systems, are the property of the County.

All systems must be used in accordance with current United States copyright laws and intellectual property rights. County employees do not have a right to and should not have an expectation of privacy while using any County equipment at any time. The County reserves the right to access, view, review, monitor, read, copy, print, disclose, delete, forward, or otherwise control any and all e-mail messages, County owned content and internet access logs or associated electronic files residing on or generated through any County system or device at any time, with or without cause or notice. This includes whether the messages, logs or files reside on the system, device or otherwise, whether the messages, logs or files are County business related or personal, and whether the messages, logs or files are sent or received. County also reserves the right to check messages, logs and files to determine whether its e-mail and internet use policy is being followed. The County retains the right to unilaterally limit access to the information technology environment for any reason.

The purpose of providing access to the internet is to support business-related activities and research by County employees. The equipment necessary to access the internet is the exclusive property of Yuma County; therefore, any access of the internet is to be used for official business purposes only. Access to the internet will be at the sole discretion of

CHAPTER I (GENERAL)

County management. The information technology services department will make access to the internet available when appropriate.

C. Permissible uses of Yuma County computer systems

In general, the use of the County's IT systems must be related to County business. Incidental or occasional personal use of the County's IT systems may occur, subject to the restrictions and warnings contained in this policy and all other policies of the County, and is allowed only when such use does not directly or indirectly interfere with the County's operation of ITS it systems, with the user's employment or other obligation to the County, and neither expresses nor implies sponsorship or endorsement by the County. Any such incidental and occasional use of the County's IT systems or devices for personal purposes will be treated the same as business related uses of the County's IT systems and devices.

D. Prohibited uses of e-mail and internet

All e-mail messages sent by users will contain a return e-mail address identifying the message as having been sent from the County e-mail system and may be considered public record. Consequently, all users are expected to send and to receive only e-mail messages that they would expect to be read by the general public. Prohibited uses include, but are not limited to, the following:

1. County network, computers, e-mail systems, or social media programs used for transmitting, retrieving or storing of any communications of a defamatory, discriminatory, or harassing nature; or materials that are obscene or pornographic unless directly related to job responsibilities.
2. Disparaging, abusive, sexually explicit, profane, threatening, illegal or otherwise offensive language or materials that would adversely or negatively reflect upon the County or contrary to the County's best interests; any illegal activities including, but not limited to piracy, extortion, blackmail, copyright infringement, and unauthorized access to any computers, electronic files or internet e-mail.

CHAPTER I (GENERAL)

3. Downloading non-business related information. Examples include streaming video of sporting events/games, streaming audio of radio programs, mp3 files, online games, web cams, social media posts, etc.
4. Uses for personal monetary gain or for commercial promotional purposes, personal email messages offering to buy or to sell goods or services.
5. Downloading from the internet, or otherwise opening, executing, sending, copying, saving or using documents or computer files of any kind in violation of copyright or other intellectual documents in violation of copyright or other intellectual property rights of third parties.
6. Downloading from the internet; receiving, opening or executing, saving, or installing and using software, programs, plug-ins or other binary files, such as ones containing the file extensions .exe or .com, in violation of copyright other intellectual property rights, or software licensing requirements of third parties, and/or that have not been approved by the County IT Department and that have not been checked for viruses or other potentially detrimental code by a procedure approved by the County IT Department.
7. Intercepting or altering another person's e-mail messages without proper authorization.
8. Composing and sending e-mail messages so they appear to be from someone else.
9. Attempting to or sending e-mail messages anonymously, or using another person's user ID or password.
10. Sharing one's account with another user.
11. Obtaining access to the e-mail messages of others when one has no substantial County business purpose for doing so (i.e., snooping).
12. Attempting unauthorized access to e-mail messages or attempting to breach any security measures on any e-mail system.

CHAPTER I (GENERAL)

13. Sending of any e-mail messages addressed to everyone on the County's e-mail system, unless you are authorized to do so.
14. Communicating confidential or sensitive County information.
15. Forwarding of any e-mail message that is marked as personal, private or confidential to anyone outside the County's e-mail system without the written permission of the original sender.
16. Forwarding of any chain letter e-mail message; or
17. Adding software or hardware to County-owned personal computers without the consent and approval of the County IT department.

E. Prohibited uses of social media

All social media posts and/or messages will be sent from an authorized County user profile and may be considered public record. Consequently, all users are expected to send and to receive only social media posts and/or messages that they would expect to be read by the general public. Prohibited uses include, but are not limited to, the following:

1. Social media posts and/or messages used for transmitting, retrieving or storing of any communications of a defamatory, discriminatory, or harassing nature; or materials that are obscene or pornographic.
2. Disparaging, abusive, sexually explicit, profane, threatening, illegal or otherwise offensive language or materials that would adversely or negatively reflect upon the County or contrary to the County's best interests; any illegal activities including, but not limited to piracy, extortion, blackmail, and copyright infringement.
3. Uses for personal monetary gain or for commercial promotional purposes, social media posts and/or messages offering to buy or to sell goods or services.
4. Intercepting or altering another person's or party's social media profile, posts and/or messages without proper authorization.

CHAPTER I (GENERAL)

5. Composing and sending social posts and/or messages so they appear to be from someone else.
6. Attempting to or sending social media posts and/or messages anonymously, or using another person's social media profile.
7. Sharing one's social media account profile with another user without authorization.
8. Obtaining access to the social media posts and/or messages of others when one has no substantial County business purpose for doing so (i.e., snooping).
9. Attempting unauthorized access to social media user profiles, posts, and/or messages or attempting to breach any security measures on a social media site.
10. Sending of any social media posts and/or messages addressed to contacts and/or other County business contacts on the user's social media profile, unless authorized to do so.
11. Communicating confidential or sensitive County information on social media.
12. Forwarding of any chain letter, social media post and/or message of a non-County business related nature.

F. Administration and oversight of social media in Yuma County

1. The creation of all County departmental social media profiles shall be approved by the agency head and County Administrator prior to activation.
2. Yuma County's social media presence shall be limited to Facebook and Twitter. Any other Yuma County social media presence and/or use of any other social media platforms are not permitted without authorization from the County Administrator.

CHAPTER I (GENERAL)

3. All social media profiles shall have at least two employee Administrators; one within the agency and one designee from County Administration's communications division.
4. All social media profiles and account activity may be monitored by a designee from County Administration's communications division.
5. The agency head shall oversee and audit their department's social media profile and activity on a quarterly basis.
6. All escalated issues occurring on social media shall be resolved by the agency head and County Administrator or designee.

Legitimate law enforcement use (e.g., those whose job requires them to track sites of an otherwise questionable nature) may exceed the guidelines within this section. For law enforcement activities, the County may choose to provide alternative internet access that is not part of the County network for the purposes of investigations and stealth. Any equipment on alternative internet access that is used for law enforcement investigations will not be subject to this policy.

G. Privacy, confidentiality and access and disclosure of e-mail messages, log of internet sites visited, social media and all associated electronic files

It is the intended purpose of this policy to limit personal use of the County's e-mail and internet systems during scheduled business hours. Users of the County's e-mail and internet systems should be aware that the County's internet access software automatically creates a log of the addresses of the internet sites visited. The County reserves the right to access information on an account or device at any time without prior notice or permission from the user, in the course of an investigation of misconduct or misuse of the e-mail or internet system, or:

1. To prevent interference with the mission of the County or department.
2. To locate substantive information required for County business.
3. To respond to legal processes.
4. To fulfill the County's obligation to third parties.
5. To respond to open public records requests.
6. To investigate a possible violation of County policy.

CHAPTER I (GENERAL)

7. To investigate a breach of the security of the e-mail system.
8. When there is reasonable suspicion that a user has committed or is committing a crime.
9. When a user is unavailable and such information is vital to County operations.
10. When a user leaves County employment for any reason; or for any other reason identified by appropriate authorities of the County.