



Administrative Manual

Title 10 PERSONNEL

Chapter 10 GENERAL POLICIES & STANDARDS

1. Electronic Systems Use—General.

Glenn County electronic equipment, software, and all information created sent or received via the equipment are the sole property of the County and/or the State of California.

Glenn County does or has the capability to and reserves the right to monitor, log and/or recover all network and PC activity with or without notice, including, but not limited to network, internet and e-mail activity and usage. Therefore users should have no expectation of privacy in their use of these resources.

Use of these systems is intended for official County business. However, some limited incidental personal use is allowed. Discretion must be exercised to ensure that personal use does not result in a direct cost to the County or hinder staff productivity. Inappropriate use could result in misuse of an employee's work time and therefore productivity, as well as an abuse of Glenn County computing resources, and may result in disciplinary action as determined by the employee's department head.

All users granted the privilege of accessing the County computing and information resources must read and sign statement acknowledging receipt and understanding of this policy. All users are expected to act in a responsible manner by complying with all policies, relevant laws and contractual agreements related to computers, networks, software, other intellectual property, and computer information.

Unauthorized use of these systems is strictly forbidden and subject to discipline under the County personnel rules (Title 10 Glenn County Administrative Code/Glenn County General Unit MOU/Glenn County Mid-Managers Association MOU/Glenn County Peace Officer Association MOU/ Glenn County Deputy Sheriff's Association MOU).

Unauthorized use includes but is not limited to:

- a. Operation or use of any system for personal, financial, or political gain.
- b. Solicitation of County employees.
- c. Operating any system in an unsafe or reckless manner.
- d. Unapproved movement or disconnection of equipment.
- e. Illegal copying or altering of software.
- f. Unauthorized deleting installed programs or data.
- g. Loading any software that is not authorized by the department head or his/her designee.
- h. Removing equipment, software, or data from department/agency premises without prior authorization.
- i. Knowingly accessing, creating or transmitting any discriminatory, offensive or unprofessional information or messages.
- j. Knowingly disseminating false information.
- k. Publishing information on the Internet unless expressly approved by the department head or his/her designee.
- l. Purchasing commercial Internet services such as America Online or Web pages designed without the approval of the department head or his/her designee.
- m. Operation or use of any system to conduct or engage in any illegal or prohibited activities, in violation of State, Federal or local laws, regulations, rules, county regulations, policies or directives.
- n. Assume another person's identity or use another person's name, unless expressly authorized by the department head or his/her designee.
- o. Distribution of protected passwords without the authorization of the department head or his/her designee.
- p. Encrypting data files without the authorization of the department head or his/her designee.
- q. Copying another employee's electronic messages, voice mail, e-mail, or other personal communication without the permission of the employee for whom the message was intended. This covers unauthorized copying by an employee, and does not in any way prohibit Glenn County management access to, or right to copy, pursuant to

Section 1 of this policy.

r. Any form of harassment.

s. Knowingly introducing malicious programs into Glenn County's networks or servers (e.g. viruses, worms, Trojan Horses, e-mail bombs, etc.)

Glenn County will not be responsible for any damages that employees may suffer from or related to their use of any County electronic information resources, including, but not limited to loss of data resulting from delays or service interruptions. Users must recognize that the use of such electronic information resources is for work-related purposes.

As information stored on portable computers (e.g. laptops and Personal Digital Assistants) is especially vulnerable and more susceptible to issues such as theft and loss, users should exercise special care in the handling, storage, and transportation of this equipment.

2. Electronic Systems and Information Assets Defined.

The following is a non-inclusive list of electronic systems, it includes, but is not limited to:

Cellular telephones

Copy machines

Data processing systems

Electronic mail (e-mail)

Electronic tablets

Facsimile machines (fax)

Internet facilities or other modem accesses

Laptops

Pagers

Personal computers

Personal Digital Assistants (PDAs)

Printers

Scanners

Servers

Shredders

Social media (e.g.: Facebook, Twitter, Instagram, etc.)

Software

Telephone system

Voice mail systems

Information assets include all data and software, whether internally developed or acquired from outside Glenn County. Information may be represented in a variety of formats, including, but not limited to:

CD Rom

Hard copy

Microfiche

Magnetic tape

Microfilm

Diskettes

Other methods of storage or transmission

Terminal display

3. Electronic Systems—Internet and Electronic Mail Communications

Glenn County electronic mail (e-mail) is provided for the purpose of conducting the business of the County.

However, as previously mentioned, limited incidental personal use is allowed. Discretion must be exercised to ensure that personal use does not result in a direct cost to the County and does not hinder staff productivity. Personal e-mail communications should be limited similar to personal phone calls, which will be discussed in the next section.

Staff shall not knowingly distribute any offensive, discriminatory, obscene or unprofessional material through the County network. Staff shall not knowingly disseminate any false or fraudulent information.

County e-mail messages are not private communications. Glenn County management reserves the right to retrieve and read any e-mail message composed, sent, or received on agency equipment, without prior notice to the employee.

E-mail is subject to the policies concerning other forms of communication, as well as all other applicable policies including, but not limited to, confidentiality, conflict of interest, general conduct and sexual harassment.

Unless a specific legal exemption applies (confidentiality), all e-mail messages, even those that have been erased, may be considered public records subject to disclosure under the Public Records Act. It is possible that persons involved in litigation with the County might also access those messages.

E-mail messages that are pertinent to departmental operations and functions must be maintained in accordance with applicable federal, state and local requirements governing the operations of the department, the same as hard copy records are maintained.

All department/agency employees and other team members should be aware that even when a message has been erased, it might still be possible to recreate the message.

External personal e-mail accounts such as Yahoo, AOL, MSN, etc. should not be accessed from Glenn County networks, without department head authorization on a case by case basis.

4. Electronic Systems—Telephones and Voice Mail

Personal calls shall be discouraged and strictly limited to those necessary to maintain the health, safety, and well being of the employee's family unit. Personal calls should not be of a social nature, only of necessity. To the extent feasible, personal calls made from the office should be undertaken during break or lunchtime. Only under exceptional circumstances should calls by employees be made when they are not on break. All long distance telephone calls must be charged to the employee's personal credit card or home telephone. Excessive incoming personal phone calls are to be discouraged.

Employees traveling on agency business are allowed one personal phone call at County expense for every twenty-four hours they are assigned to be out of the County. Said call(s) shall be reasonable in duration. The employee may be liable for payment of phone calls that exceed the above-mentioned limit or are excessive in duration. This policy does not apply to hotel access charges. The County shall consider these charges, if not excessive, to be a legitimate business expense.

Cellular phones may be assigned to Glenn County department/agency team members who have a clear business need. Cellular phones are to be used for County business only, when necessary in the performance of job duties. County employees may privately purchase a second line for the County cellular phone for personal use.

Glenn County department heads have the authority and responsibility to limit inappropriate or excessive personal use of telephones.

Voice mail messages should be limited to County business. Voice mail should not be used for conducting outside business pursuits. However, messages which are necessary to maintain the health, safety, and well being of an employee and their family are acceptable.

5. Social Media

Social Media websites, e.g.: Facebook, Twitter, Youtube, etc., have become a part of our everyday lives. To address the fast-changing landscape of the Internet and the way residents communicate and obtain information online, Glenn County departments may consider participating in social media to reach a broader audience. Glenn County supports the use of social media to further the goals of the County and the missions of its departments where appropriate. Glenn County endorses the secure use of social media tools to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity improvements. However, their application must not compromise data confidentiality and integrity. This policy establishes guidelines for the use of social media.

A. Purpose:

This policy establishes consistent standards for, and ensures appropriate use of, Social Media administered by employees and agents representing the County of Glenn. For the purpose of this policy, the term "Social Media"

refers to media that allow users to collaborate and share information with a network of other users or the community as a whole, including but not limited to Facebook, Twitter, and Youtube, and text messaging.

B. Scope:

This policy applies to all Glenn County sponsored social media sites, and social media use by County employees. This policy is not intended to regulate the personal activities of Glenn County employees or contractors with respect to the use of social media. A Glenn County sponsored social media site is one designed and administered by a Department to represent the Department in an official capacity.

C. Policy:

- (1) All official Glenn County presences on social media sites are considered an extension of the County's network and subject to all related administrative policies, including but not limited to policies on computer use.
- (2) Only authorized individuals shall have permission to create, publish or comment on behalf of the County of Glenn on County sponsored Social Media sites.
- (3) The official websites for County of Glenn remains the County's primary and predominant Internet presence.
- (4) Content on County of Glenn-Sponsored Social Media sites shall not be offered in lieu of official information on the County's official website, except when immediate and temporary disclosure of information is appropriate.
- (5) County of Glenn-Sponsored Social Media sites shall contain a link back to the County's official websites, where the announcement, press release, form(s), document(s), online services and/or other information relevant to the matter shall be posted.
- (6) County of Glenn-Sponsored Social Media site posts are a public record subject to disclosure under the California Public Records Act (Government Code §§ 6250 to 6270). Therefore, all Social Media content must be archived and managed in accordance with the applicable records retention schedule.

D. Public Comments:

- (1) Employees and contractors maintaining County of Glenn-Sponsored Social Media sites that permit public comment shall inform visitors of the intended purpose of the site and provide a clear statement of the discussion topic introduced for public comment so that the public is aware of the limited nature of the discussion and notified that inappropriate posts are subject to removal, including but not limited to the following types of postings, regardless of format (text, video, images, links, documents, etc.):
 - a. Comments not topically related;
 - b. Profane language or content;
 - c. Content that promotes, fosters or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regards to public assistance, national origin, physical or mental disability or sexual orientation;
 - d. Sexual content or links to sexual content;
 - e. Solicitations of commerce;
 - f. Conduct or encouragement of illegal activity;
 - g. Information that may tend to compromise the safety or security of the public or public systems; or content that violates a legal ownership interest of any other party.
- (2) Employees and contractors maintaining County of Glenn-Sponsored Social Media sites that permit public comment shall prominently display, or provide a link to, the below Comment Policy on each online page that displays discussion content.

E. Content of Posts:

- (1) Employees and contractors using Social Media to communicate on behalf of a County of Glenn on a County of Glenn-Sponsored Social Media site should be mindful that statements posted represent the County of Glenn, including its elected officials. Therefore, employees and contractors should use discretion before posting.
- (2) Posts should be designed to increase the public's knowledge, trust, and use of County services.
- (3) Posts should always relate to matters within the scope of the County of Glenn's function and should be consistent with the County's public service mission.
- (4) To help distinguish County of Glenn-Sponsored Social Media sites from non-official (or personal) uses of these tools, County sponsored Social Media sites must state that they are maintained by the County and that they are subject to the County's Social Media Policy.
- (5) County of Glenn-Sponsored Social Media sites must identify the department responsible for the information displayed, including all descriptions, logos, images, etc. representing County of Glenn services.
- (6) Confidential or non-public information must not be shared.
- (7) Postings must respect copyright laws and reference or cite sources appropriately.
- (8) Only information authorized under this Policy shall be posted.
- (9) Employees and contractors must not use County sponsored Social Media sites for political purposes or to conduct private commercial activities, except as such uses are specifically permitted by the Glenn County Board of

Supervisors. For this reason, links to political or commercial websites are prohibited, unless the Glenn County Board of Supervisors specifically permits such links.

F. Responsibilities

- (1) County of Glenn Department Heads and designees are responsible for:
- (2) Managing the department or County's site(s) in a manner consistent with this Policy, including content monitoring;
- (3) Granting authority to specific individuals to post content on the department or County's Social Media site(s) while ensuring that posts aren't made by unauthorized representatives;
- (4) Maintaining a list of Social Media sites hosted by the department or County, active account logins and passwords;
- (5) Changing passwords periodically and when an individual is removed as an administrator; and
- (6) Ensuring that all authorized representatives read the Policy for Official Use of Social Media Sites and sign the acknowledgment form signifying that they agree to follow the Policy and all related standards and guidelines
- (7) A County of Glenn department may develop a supplement to append to this Policy that includes policies or procedures unique to systems or services specific to that department, provided that such supplements shall not be less restrictive than this Policy. All such supplements must be reviewed and approved by the County Information Services Committee for consistency with applicable technical policies and standards.

6. Electronic Systems--Information Safeguards

All information maintained by Glenn County departments/agencies is considered an asset of the County and shall be protected from damage, loss, misuse, or inappropriate disclosure. Management is responsible for administering adequate controls to ensure the security, confidentiality, and integrity of information. Glenn County employees are required to maintain proper levels of protection for information assets.

Managers and supervisors are responsible for those Glenn County information assets that are held within their department. Individual managers and/or employees may be assigned custodial responsibility at the department or application system level to ensure accuracy, integrity, security, adequate controls, and confidentiality of agency information assets.

Where proprietary software or property has been provided to the County under confidentiality agreements, it is the responsibility of the department/agency to ensure compliance with the terms of such agreements.

Employees or other department/agency team members who disclose, alter, or willfully destroy information that adversely impacts County services, or who violate copyright laws will be subject to applicable federal, state, and local criminal laws, as well as to disciplinary action pursuant to County policies and procedures.

Each Department is responsible for designating an individual who will be responsible for approving staff access to County networks, internet, e-mail, etc. Including but not limited to:

- a. Approving and revoking access to County networks, internet, and e-mail, when appropriate. The level of access granted will be determined by the employee's immediate supervisor or manager. This should be accomplished and documented through the use of a system access form.
- b. Determining appropriate activities of staff on the County network and internet.
- c. Investigate suspected non-compliance with this policy and determining what corrective actions should be taken.

All computers connected to the County network must continually execute approved virus-scanning software with a current virus database.

7. Passwords

a. Overview

Passwords are essential to system security. Passwords provide one layer of security for access to data residing in the Glenn County information systems infrastructure. Passwords must meet a minimum standard of complexity to ensure Glenn County information systems and resources are protected from exploitation.

b. Purpose

The guidelines listed below are the minimum standard required by all information systems under Glenn County. This policy is not intended for departments that must conform to HIPAA, PII, or HITECH. Individual departments under the constraints of HIPAA, PII, or HITECH must have an internal policy to meet these standards.

c. Scope

This policy pertains to all personnel that have or are responsible for an account (or any form of access that supports or requires a password) for any system that resides at any County facility, has access to the County network, or stores any non-public County hosted/stored information.

d. Policy

General Guidelines

(1) All system-level password (Service Accounts, System Accounts, Any account not logged into by a user) must meet the minimum password standard as follows:

(a) 12 characters in length (minimum)

(b) Two out of three (minimum): Special Character (Include, but are not limited to: !@#\$%^&*()_-+=?.,''";<>[]{})), Uppercase Letter, Number

(c) Must be changed upon the termination of any employee with Domain Administrator access to the information systems infrastructure.

(2) All Domain Administrator level accounts (IT Administrators, Contracted IT staff) must meet the minimum password standard as follows:

(a) 10 characters in length (minimum)

(b) Two out of three (minimum): Special Character1, Uppercase Letter, Number

(c) Must be changed every 45 days

(3) All User accounts (accounts with system access) must meet the minimum password standard as follows:

(a) 8 characters in length (minimum)

(b) Two out of three (minimum): Special Character1, Uppercase Letter, Number

(c) Must be changed every 90 days

(d) Must be unique to the end user and not a password assigned by IT staff

(4) All endpoint devices that have access to Glenn County information systems (Mobile Phones, Tablets, etc) must meet the minimum password standard as follows:

(a) 4 characters in length

(b) May contain numbers or letters

(5) All passwords must be different than the previous 6 passwords.

(a) This guideline is enforced by IT Administration

(6) All system passwords must be changed from their default password

(7) County system passwords should not be used for external accounts. For example:

(a) DSL Accounts

(b) Web based email accounts

(8) All passwords, if written down or stored

(a) Must be stored in a secure location:

♣ Locked file cabinet

♣ On your person

♣ Secured network location (Is any location on the network that only that individual has access and it must require a password to get to the location)

(b) Do not share your County passwords with co-workers.

(c) Here is a list of things to avoid:

♣ Talking about a password in front of others.

♣ Hinting at the format of a password (e.g., "my family name").

♣ Writing in your password on questionnaires or security forms.

♣ Sharing your password with family members.

♣ Telling your co-workers your passwords while on vacation.

• Never use the "Remember Password" feature of applications (e.g., Internet Explorer, FireFox).

(9) If a password is suspected to be compromised

(a) Password must be changed immediately

(b) Incident must be reported to IT personnel or security officer

(c) An investigation of activities may be performed on the account in question

(10) Staff Termination

(11) Accounts must be disabled immediately

Violators of this policy may be subject to disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

8. Confidential Information

Communication on the internet is not secure and should be used accordingly. Users are warned that any confidential information sent through the Internet or e-mail could be intercepted, modified, misdirected or destroyed by unauthorized persons if adequate access controls are not in place.

When sending confidential information through e-mail users should:

- a. Have a compelling reason for sending confidential information and take every precaution to ensure the security of the information.
- b. Prior to sending confidential information, users should also confirm the correct e-mail addresses of the intended recipients.
- c. Include the word CONFIDENTIAL in the subject line of the message.
- d. Never include any confidential or sensitive information in the subject line of the e-mail.
- e. Include a disclaimer such as the following in the body of the e-mail message:
"This electronic message may contain information that is confidential and/or legally privileged. It is intended only for the use of the individual(s) and entity named as recipients in the message. If you are not an intended recipient of the message, please notify the sender immediately and delete the material from any computer. Do not deliver, distribute, or copy this message, and do not disclose its contents or take action in reliance on the information it contains. Thank you."

Encryption of e-mail is appropriate in some instances to secure the contents of an e-mail message. Each user should be cognizant of the sensitivity of information contained in e-mail.

9. Copyrighted Material

Users may download copyrighted material, but its use must strictly be within the limitations posed by the author or current copyright law. The Federal Copyright Act at 17 U.S.C. 101 et seq. protects "intellectual property" rights and prohibits misuse of all original works of authorship in any tangible medium of expression.

It is against County policy to download any information in violation of copyright laws. This includes, but is not limited to music, movies, pictures, etc.

10. Public Domain Material

Any user may download public domain images, documents, etc. for County business use, but does so with the knowledge that by doing so, the employee assumes all risks regarding whether or not the material was in the public domain.

11. Downloading

Users are reminded of the potential dangers associated with downloading information from the Internet, such as the possibility of exposing the County network to Viruses, Worms, Trojan Horses, Spyware, etc. which may be spread through downloaded software and files.

Users shall consult their Department's policies and procedures prior to downloading information from the internet. Users should download information from trusted sites, when possible.

The downloading of any executable software is prohibited unless done with case by case knowledge and approval of the department head or his/her designee.

12. Electronic Systems – Policy Violation Notification

An employee or team member learning of violations of this policy should notify his/her manager or supervisor as soon as possible.