MARICOPA COUNTY SHERIFF'S OFFICE POLICY AND PROCEDURES

Subject

ELECTRONIC COMMUNICATIONS, DATA AND VOICE MAIL

Policy Number
GM-1

Effective Date
03-07-24

Related Information

ARS 38-1104
CP-2, *Code of Conduct*
GC-17, *Employee Disciplinary Procedures*
GD-9, *Litigation Initiation, Document Preservation, and Document Production Notices*
GD-23, *Employee Access to the Internet/Intranet*
GE-3, *Property Management and Evidence Control*
GF-3, *Criminal History Record Information and Public Records*
GH-2, *Internal Investigations*

Supersedes

GM-1 (01-12-22)

PURPOSE

The purpose of this Office Policy is to provide employees guidelines and procedures regarding the appropriate use of Maricopa County Sheriff's Office e-mail, voice mail, and other electronic communications, to promote efficient and convenient ways of conducting Office business.

Although this Office Policy refers to employees throughout, this Office Policy also applies with equal force to all volunteers. Volunteers include, but are not limited to, reserve deputies and posse members.

POLICY

It is the policy of the Office to establish procedures and responsibilities for Office employees regarding the use of Office e-mail, voice mail, and other electronic communications.

DEFINITIONS

Electronic Communications: Messages that are transmitted or received by electronic means through the Office and/or Maricopa County issued equipment, such as e-mail, voice mail, instant messaging, Microsoft Teams for business, Computerized Aided Dispatch (CAD) instant messaging, text messages, and all data passed through the Office network, the Internet, Intranet, ticketing system, personal data assistant (PDA), iPhone, evolution data optimized (EVDO), or virtual private network (VPN).

Electronically Stored Information **(ESI)*:*** Information that is created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. ESI may be stored on and retrieved from many sources, including computer hard drives, network servers, flash (USB) drives, databases, cloud storage, mobile devices, such as mobile phones and tablet computers, which may include County-issued devices or personal devices, and social media websites. Common examples of ESI include word processing documents, spreadsheets, digital photographs, videos, e-mails and their attachments, text and instant messages, call logs, voicemails, and databases.

E-mail: Any transmission of messages, including attachments and embedded objects, across the Office network by electronic means, such as commercial and electronic mail applications, operating system messaging capabilities, and Internet mail.

Employee: A person currently employed by the Office in a classified, unclassified, contract, or temporary status.

Formal Communications: Messages and documents transmitted or received by e-mail that obligate the receiver to implement or change any activity or procedure relating to the delivery of services to the public, or that convey the acceptance or implementation of contracts, bids, or other agreements binding on Maricopa County or its employees, or the acceptance of any financial obligation on behalf of Maricopa County.

Logical Security: An intangible process that identifies, authenticates, authorizes, and provides access control over programs and data, such as a password.

Personal Electronic Device: A personally owned device which may include, but is not limited to, a cellular phone, laptop computer, USB, camera, voice recorder, or home computer.

Physical Security: Material factors such as environment, communication wiring, or devices such as a lock.

Routine E-mail: Communications having to do with matters such as the scheduling of meetings; notification of legal or policy issues, requests for information, advice, assistance, direction, or instructions, or other notifications, such as employee absences.

Voice Mail: An electronic communication system in which spoken messages are recorded or digitized for later playback.

Volunteer: A person who performs hours of service for civic, charitable, or humanitarian reasons, without promise, expectation, or receipt of compensation for services rendered. An employee may not volunteer to perform the same, similar, or related duties for the Office that the employee is normally paid to perform.

PROCEDURES

1. **Use of Office or Maricopa County Equipment:**

   A. Employees shall use Office and Maricopa County equipment for its intended purpose. Limited incidental personal use of Office and Maricopa County telephones, cellular phones, and computers is permitted, provided that use does not inhibit governmental or administrative use, impact network bandwidth, storage, availability or security, or impact an employee's ability to perform their assigned duties.

   B. Office and Maricopa County equipment shall not be used in a manner that discriminates or denigrates anyone on the basis of age, nationality/national origin, immigration status, religious beliefs/religion, race, color, gender, culture/cultural group, sexual orientation, gender identity/expression, veteran status, ancestry, physical or mental disability, ethnic background, or socioeconomic status.

   C. Social networking sites shall not be accessed on Office equipment while on-duty unless in the performance of official duties or accessing official Office controlled social media sites for viewing purposes of Office announcements only, as specified in Office Policy CP-2, *Code of Conduct*.

   D. Employees are prohibited from accessing the TikTok social media application on all Office controlled devices. Employees are also prohibited from accessing the TikTok social media application on a personal controlled electronic device that is connected to the Office, or the Maricopa County courts Wi-Fi or direct network, as specified in Office Policy CP-2, *Code of Conduct*.

2. **Electronic Communications:** This Office Policy is not intended to conflict with or supersede the guidelines established for the use of the Office Internet/Intranet, as specified in Office Policy GD-23, *Employee Access to the Internet/Intranet.* Employees are cautioned to use discretion and good judgment when sending electronic communications or voice mail messages. All electronic communications shall be professional in content and shall not be used in a manner that discriminates or denigrates anyone, regardless of age,

nationality/national origin/ immigration status, religious beliefs/religion, race, color, gender, culture/cultural group, sexual orientation, gender identity/expression, veteran status, ancestry, physical or mental disability, ethnic background, or socioeconomic status.

A. Office employees should be aware that electronic communications and voice mail messages are capable of being forwarded, monitored, or read by someone other than the intended recipient. Employees should not harbor any expectations of privacy regarding their electronic communications. Messages should be edited appropriately.

1. Personnel shall refrain from using profane or offensive language or images in any aspect of their electronic communications, including system passwords.

2. Electronic communications are in most instances considered public records and may be obtained by members of the public through a request for information.

B. To the full extent permitted by applicable law, the Office reserves the right to search and otherwise gain access to an employee's electronic communications, calendar, data stored on Office devices, servers, personal devices if used for Office business, and voice mail messages whenever it is deemed necessary for business or supervisory reasons, with or without advance notice.

1. The respective bureau chief shall review and approve any requests for access to the contents of an employee's electronic communications data stored on Office devices, servers, personal devices if used for Office business, and voice mail messages, unless otherwise authorized in writing by the Chief Deputy, the request is made by the Bureau of Internal Oversight (BIO), the Legal Liaison Section (LLS), or by the Professional Standard Bureau (PSB) during the course of an investigation.

2. Any access undertaken, other than as set forth in paragraph one above is prohibited.

3. **E-mail, Instant Messaging (Microsoft or Others) and Voice Mail Provisions:** E-mail, instant messaging, and voice mail are communication tools used by the Office to convey information such as policy and procedural updates, daily operational activities, and announcements.

A. The use of non-business-related background images, graphics, stationary or themes in e-mails is prohibited.

B. The use or forwarding of multiple messages, chain mail, SPAM, offensive material, or non-Office related messages is also prohibited.

C. When employees are on duty, they are responsible for checking their e-mail and voice mail on a daily basis, or as specified by their supervisor.

D. Voice mail and e-mail systems shall normally be used for routine Office business only. However, employees may make limited use of the voice mail and e-mail systems under the following circumstances:

1. Scheduling of personal appointments as an effective extension of overall time management.

2. Sharing of event driven information and planning of work-related social events where the intent is to enhance employee morale.

3. Other limited uses that are not disruptive, offensive to others, harmful to morale, or solicitous of others for a non-work-related activity.

4. Other than the limited use exemptions identified in this section, or for official Office purposes, the use of the Office e-mail address to subscribe to commercial vendors or entities, or to receive e-mail notifications from commercial vendors or entities, is prohibited.

E. Employees are responsible for taking reasonable precautions to safeguard their voice mail, instant messaging, and e-mail from unauthorized entry or use.

1. Employees shall not engage in any practice that compromises existing physical and logical security measures. The following are examples of compromising behavior:

a. Leaving a document of a sensitive nature displayed on a computer screen when not working on the document. Employees must lock their devices when stepping away from their workstation.

b. Attempting to open, retrieve, or otherwise gain access to information or data on any computer system which the user does not have authorization to access.

c. Allowing others to know personal system passwords and security codes.

2. Employees shall promptly notify the Sheriff's Office Technology Management Bureau Operations Center of any changes or problems with physical or logical security for their voice mail or e-mail, to request changes, password resets, and to report personnel changes.

3. Employees shall keep personal log-ons and passwords confidential and change their passwords on a regular basis as recommended or required.

a. Passwords shall be changed from the initial default.

b. Employees should not choose passwords based upon personal data such as their name, date of birth, serial number, or other information that another person could easily obtain and use.

c. Passwords must meet complexity requirements:

(1) Must be a minimum length of eight characters;

(2) Must not be the same as the username/user ID;

(3) Must expire and be changed within a maximum of 90 calendar days; and

(4) Must not be identical to the previous 10 passwords.

d. Passwords for voice mail, such as a PIN number, should not be the last four digits of an employee's office telephone number.

4. **Management of E-mail and Voice Mail:** Office employees are solely responsible for the management of their voice mail and e-mail mailboxes and any associated folders.

A. Information on the voice mail or e-mail system should be current or pertinent.

1. Current or pertinent information may be saved in an appropriate folder in the e-mail system, in the voice mailbox, as a Word document, in OneNote, or other MCSO-provided technology.

a. In the event a Document Preservation Notice is filed, an employee's Electronic Stored Information (ESI) shall be preserved, as specified in Office Policy, GD-9, *Litigation Initiation, Document Preservation, and Document Production Notices*. Communications subject to an existing *Document Preservation Notice* shall be preserved in the appropriate e-mail file or in its original format.

b. Formal communications transmitted or received through e-mail shall be printed and preserved in the appropriate file in paper format pursuant to the Office Retention and Disposition Schedule. Once these communications have been preserved as specified, they may be deleted from the system.

c. Routine e-mail may be deleted after being read and any required action taken, unless there is a *Document Preservation Notice* that specifies other retention or preservation requirements, as specified in Office Policy, GD-9, *Litigation Initiation, Document Preservation, and Document Production Notices*.

2. When an employee empties their deleted folder and logs off properly, the message is removed from the Outlook account.

a. The message is retained by the e-mail system for 28 days and can be recovered by the Technology Management Bureau during that time.

b. After 28 days, the message is permanently deleted from the e-mail system, but if circumstances require, it may be recovered by the Technology Management Bureau.

c. In the event a Document Preservation Notice is filed, an employee's e-mails associated with the Document Preservation Notice shall not be deleted and shall be preserved, as specified in Office Policy GD-9, *Litigations Initiation, Document Preservation, and Document Production Notices*.

3. Voice messages remain on the system until deleted by the user or they are deleted automatically following the specified message retention period. When a user deletes a message and logs off properly from the voice messaging system, the message is permanently erased by the system.

B. Recorded greetings on the voice mail system, to include Office issued cellular phones, shall be current, non-generic, and informative. The following information shall be contained in a recorded greeting:

1. Employee's name.

2. Specialized information, such as an extended vacation or an alternative contact number.

C. Exceptions to this requirement shall only be approved by the division commander.

5. **Electronic Mail Signature:** Employees may use an e-mail signature at the end of their e-mail to provide contact information.

A. E-mail signatures are restricted to business related information and shall not contain non-business-related information such as quotations, embedded images, or any other information that may be deemed inappropriate.

B. E-mail signatures should be configured to the standardized Office eSignature template to maintain brand and graphic consistency, as follows:

MARICOPA COUNTY
SHERIFF'S OFFICE

Employee Name
Position Title
Section, Division
Bureau
Maricopa County Sheriff's Office
Street Address, Phoenix, AZ 85003

Office : 602-XXX-XXXX
Cell : 602-XXX-XXXX
E-mail :

6. **Release of Information:** Criminal History Record Information (CHRI) and information regarding sensitive criminal justice operations shall be disseminated, as specified in Office Policy GF-3, *Criminal History Record Information and Public Records*.

7. **Access to Electronic Communications by Former Employees:** Former employees shall have no right to retrieve or otherwise access the contents of electronic communications or voice mail messages.

8. **Use of Personal Electronic Devices:** Personal electronic devices to conduct Office business are not authorized unless exigent circumstances exist. Employees shall notify their supervisor if a personal electronic device is used. Exigent circumstances include the sum of the conditions and information available in any event which, taken in totality, dictates a need for immediate action. Personal electronic devices include, but are not limited to, personally owned cellular phones, lap top computers, USBs, cameras, voice recorders, and home computers. Employees who use their personal electronic device, to conduct Office business do so based solely on choice and at their own expense. Personal electronic devices used for Office business are subject to disclosure for public records requests, discovery requests, and in any administrative, civil, or criminal proceedings, as specified in this Office Policy.

   A. Employees who conduct Office business on a personal electronic device must download the information by the end of shift to an Office CD/DVD, USB, or forward the information to an Office-provided Microsoft 365 account. All Office business forwarded from a personal electronic device or e-mail account shall be deleted and purged from the personal electronic device or e-mail account once it is forwarded to an Office Microsoft 365 account.

   B. Office business such as, but not limited to, crime scene photographs, recorded interviews, and written reports, must be removed from the personal device once downloaded to an Office CD/DVD, or USB or forwarded to an Office-provided Microsoft 365 account. All Office business forwarded from a personal electronic device or e-mail account shall be deleted and purged from the personal electronic device or e-mail account once it is forwarded to an Office Microsoft 365 account.

   C. Any information received from the Arizona Criminal Justice Information Systems (ACJIS) that is downloaded to an Office or personal CD/DVD or USB, shall be stored in accordance with Arizona Criminal Justice Information System (ACJIS) requirements, as specified in Office Policy GF-3, *Criminal History Record Information and Public Records*. Digital evidence downloaded from a personal device shall be stored, as specified in Office Policy GE-3, *Property Management and Evidence Control*.

D. This section does not apply to the use of personally owned electronic devices when an employee records their own administrative investigation interview. These recordings are personal recordings and are not considered official Office business. These types of recordings are authorized, as specified in Office Policy GH-2, *Internal Investigations*.

9. **Disciplinary Actions:** Employees found to be in violation of this Office Policy may be subject to disciplinary action, up to and including dismissal from employment, as specified in Office Policy GC-17, *Employee Disciplinary Procedures*.