

# Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

## GENERAL PRINCIPLES

Technology has significantly expanded opportunities to enhance communication, efficiency, effectiveness, and productivity in the delivery of City services. The City recognizes that the use of e-mail and computers by City employees has increased significantly, raising numerous policy issues with respect to communication, creation of information and systems, retrieval and storage of records, and proper etiquette.

Technology has also greatly expanded opportunities to communicate with friends and family through email and the internet, as well as providing opportunities to conduct personal business, including shopping, social networking, online banking and other non-work activities. However, the special ethical considerations of public service require us to separate our personal lives from our professional lives.

The City's policy regarding the use of e-mail, internet services, and other electronic media is below.

## POLICY

### 1. General Policy

As stated in the Code of Ethics, City employees and officials shall not use City time, City funds, City facilities, equipment, or supplies for personal use or personal gain. This includes computers, internet access, and email. These resources are provided for City business only.

It is the policy of the City of San José that the use of City computer equipment, electronic facilities and electronic data is limited to **official City purposes** only. Employees must use the information systems for City of San José business only. Amongst other non-City related uses that are prohibited, the e-mail system may not be used to solicit or persuade others for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

Electronic mail and information systems of the City are not to be used in a way that may be disruptive, offensive to others, or harmful to morale. For example, the City prohibits the display or transmission of sexually explicit images, messages, cartoons, or any transmission or use of e-mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious or political beliefs.

Employees should use personal cell phones/smartphones or personal laptops for personal business instead of using City equipment/resources. (For hourly employees, even when using personal equipment, any personal business should be conducted during breaks or lunch periods and for salaried employees shall not interfere with work. Such use must comply with other City policies, including the Discrimination and Harassment Policy.)

From time to time, however, employees may need to use City equipment to communicate work schedule changes or scheduling or rescheduling of medical appointments because of work

## Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

schedules. For purposes of this policy, these limited and brief communications shall be considered work-related.

Because use of the City's email and internet are for City business purposes only, **employees should have no expectation of privacy when using these technologies. Email and internet use may be reviewed at any time.**

Technology in the computer and e-mail industry changes rapidly and references to named suppliers in this policy are subject to change without prior notice and modification to the policy. It is understood this policy will continue in full force and effect even if there are future additions and/or deletions to the named suppliers in this policy, if those suppliers are providing the same or similar services.

The following policies apply to the use of e-mail, internet services and other electronic media by City employees or users of the City electronic systems:

### 2. Public Records

All City records, regardless of media or format and including e-mail messages and other electronic records are governed by the requirements of the California Public Records Act (CPRA). Requests for information under the authority of the CPRA that involve e-mail messages and/or attachments should be handled in accordance with standard City and departmental policies. The City's [Public Records Policy and Protocol](#) provides guidelines regarding the CPRA and responses to requests for records under its authority.

### 3. Retention Guidelines for Electronic Records

- A. This section provides guidelines for the automatic deletion of stored items, such as emails, files and chat logs, from the City's organization-wide technology systems. For many of the technology systems it administers, the Information Technology Department (ITD) has the ability to set rules within the system for the automatic deletion of stored items after set time periods. The purpose of setting automatic deletion rules is to make efficient use of the City's electronic storage resources. The guidelines, set out in the matrix in section C below, shall inform ITD in setting the timelines for automatic deletion in the listed systems.
- B. Automatic deletion rules shall not impair compliance with the CPRA, the [Public Records Policy and Protocol](#), the City records retention schedule, or any other applicable law or policy. ITD shall have the discretion to set automatic deletion policies for a longer period than listed in the guidelines or to suspend them altogether for any individual employee, type of file, City department, or other category as may be necessary to comply with applicable law or policy, or to meet the City's business needs.

## Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

C. The retention guidelines matrix is as follows:

System	Retention Guideline	Reference Section of this Policy for Additional Guidance
Outlook for Active Employees	Outlook email should be deleted after two years, with the exception of email stored in personal folders in Outlook.	4
Outlook for Departed Employees	Outlook email for departed employees should be deleted two years after each employee's departure.	4
SharePoint	Files in the SharePoint system should be deleted after ten years.	5
OneDrive for Active Employees	Retention of files in OneDrive will be managed by individual employees and shall not be deleted according to a central policy.	5
OneDrive for Inactive Employees	OneDrive files for inactive employees should be deleted ninety days after the employee's departure.	5
Teams Chat	Teams chat messages should be deleted after three days.	6
Teams Channel	Teams Channel chat messages should be deleted after two years and one month.	6
Zoom	All meeting notes should be retained for two years.	6

#### 4. Retention and Management of E-Mail Messages

- A. The City e-mail system is not a recordkeeping system and is not intended for regular retention of e-mail. All e-mail messages and attachments that fall under the description of any records series listed on an approved City records retention schedule must be removed from the e-mail system and retained as records. The City Public Records Manager can provide advice on whether or not particular e-mails constitute records.
- B. Any e-mails and attachments that must be retained as records shall be saved as electronic files situated on the City's computer network. No e-mails or other electronic records shall be stored on desktop or laptop computer hard drives (i.e., "C drives") or in personal (.pst) e-mail files.
- C. E-mail messages and attachments that do not need to be retained as records should be deleted as soon as possible. E-mail messages on the City e-mail system may be deleted regularly and automatically from the system by ITD. This includes messages and attachments maintained in personal (.pst) files.

## **Use of E-Mail, Internet Services, and Other Electronic Media**

**1.7.1**

- D. The City Attorney's Office and/or the Office of Employee Relations may suspend the deletion of any e-mail that may be needed as documentation in the course of legal and/or disciplinary proceedings.
- E. Employees must transfer messages and/or attachments that must be retained as records to storage off the e-mail system selectively as individual files. Employees shall not transfer undifferentiated e-mail in bulk to the City's computer network or to local hard drives.
- F. Messages and attachments that are removed from the e-mail system for retention as records must be retained in accordance with an applicable approved records retention schedule. If unsure how to identify and use the applicable retention schedule, employees should contact their departmental Records Administrator or the City Public Records Manager for assistance.
- G. The Administration will implement an onboarding procedure to ensure that employees are informed of the proper retention and management of emails.
- H. Before the departure of an employee with an email account, any email in the departing employee's account that must be retained as records shall be saved as electronic files situated on the City's computer network.
- I. The City does not back-up the e-mail system on a long-term basis or for recordkeeping purposes. The City stores electronic mail only to the degree that allows the restoration of current electronic mail in the event of a systems failure. E-mail messages and attachments that have been deleted by a user prior to a periodic back-up will not be recoverable from that back-up.
- J. Each user is provided with a limited amount of storage space on the e-mail system as determined by ITD according to available resources and technological developments. When employees reach that limit, the system will not permit the user to send or receive messages until the volume of messages for the user's account has decreased within its prescribed limit.
- K. ITD will limit the size of e-mail attachments that will be permitted to be transmitted according to available resources and technological developments.

### **5. Retention and Management of Files in Electronic File Systems**

- A. Any SharePoint site that needs longer retention for compliance or business reasons will need to have a retention plan that explains why longer retention is needed and set an individual policy for the site that implements the longer timeline. IT may store any files retained longer than 10 years in a lower cost storage option.
- B. OneDrive may be used to draft files before they're ready to share but should not be used to store files after the work product is complete. SharePoint should be used for

## **Use of E-Mail, Internet Services, and Other Electronic Media**

**1.7.1**

that purpose.

- C. The Administration will implement an onboarding procedure to ensure that employees are informed of the proper uses of OneDrive and SharePoint. It will also implement an offboarding procedure to ensure that any records with retention requirements maintained in OneDrive at the time of an employee's separation are transferred to SharePoint.

### **6. Retention and Management of Messages in Electronic Collaboration Platforms**

- A. All Teams Chat messages that fall under the description of any records series listed on an approved City records retention schedule must be removed from the Teams Chat system and retained as records. The City Public Records Manager can provide advice on whether or not particular messages constitute records.
- B. The Administration will implement an onboarding procedure to ensure that employees are informed of the proper use of Teams Chat.
- C. Teams Channel messages deleted after two years and one month instead of two years because Teams Channel is often used by departments during emergency management exercises, which take place on a two-year basis. Allowing an extra month makes it possible for departments to refer to records of the previous exercise before conducting the next one.

### **7. Privacy, Access, and Ownership of E-Mail**

Messages sent and received via the City's e-mail system are the property of the City. The City reserves the right for any reason to access and disclose all messages and other electronic data sent over its electronic mail system or stored in its files. The City has the right to delete or retain any or all electronic files including e-mail of a City employee who is no longer employed by the City. **There are no rights to privacy when using the City's e-mail and internet system.**

Departments that want to access a current employee's email or internet access, must receive written approval from the City Manager's Office, by submitting a request to the City Manager's Office of Employee Relations. A Department Director or designee must approve access to a former employee's email or internet access.

### **8. Attorney-Client Privileged Communications and Attorney Work Product**

Some messages sent, received, or stored on the City e-mail system will constitute confidential, privileged communications between the City and its attorneys. Some messages may be subject to the attorney work product doctrine as well. Attorney-client communications and attorney work product should never be forwarded without consulting both the City Manager's Office and the City Attorney's Office.

## Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

### 9. Confidential Information

Most communication among City employees is not considered confidential. However, certain communications, such as police investigations and personnel records, may be confidential or contain confidential information. Questions about whether communications are confidential should be raised with the City Manager's Office or City Attorney's Office.

- A. Employees shall exercise caution in sending confidential information on the e-mail system as compared to written memoranda, letters, or phone calls, because of the ease with which such information may be retransmitted.
- B. Confidential information should not be sent or forwarded to individuals or entities not authorized to receive that information and should not be sent or forwarded to other City employees not directly involved with the specific matter.
- C. Care should be taken in using e-mail to ensure messages are not inadvertently sent to the wrong individual. In particular, employees should exercise care when using distribution lists to make sure all addressees are appropriate recipients of the information. Lists are not always current and individuals using lists should take measures to ensure lists are current.
- D. Confidential information sent to non-City email accounts should be fully secured with encryption (mechanism to convert information into code to prevent unauthorized access. ITD should be contacted in the event that any assistance is needed with encryption). This includes Personally Identifiable Information, Credit Card Information, Protected Health Information, and any other type of confidential data.
- E. Employees shall not discuss confidential information outside of the workplace.
- F. Confidential information should not be reproduced unnecessarily.
- G. Employees shall return all tangible forms of confidential information to the City upon termination of employment or at the City's request.

### 10. Internet and Intranet Services

The City of San José provides employees with Internet and Intranet access for official City business purposes only. The following policies are applicable to employee use of the Internet or Intranet via City provided access:

- A. The City reserves the right to deny internet and/or intranet access to any employee or group of employees.
- B. Employees shall not create discussion groups (blogs) on the Internet or Intranet without approval from the Department Director and the City Manager's Office.

## Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

- C. Departments shall designate a 'Content Manager' for point of contact with (ITD) and the City Manager's Office.
- D. Departments shall use the City's Internet home page for all Internet postings and Intranet home page for Intranet postings, and shall not initiate new or separate services outside of the City's designated services without the consent of the Department Director and the City Manager's Office. Internet and Intranet home pages external to the City's official sites must be linked to these home pages.
- E. Departments shall post information to the Intranet and Internet using guidelines provided by the City Manager's Office.
- F. The decision of the City Manager's Office for appropriateness of materials and usage of Internet and Intranet services shall be final.
- G. Department Directors have primary responsibility to ensure adherence to this policy.
- H. ITD has technical responsibility for setting up and managing Internet and Intranet resources, including user account maintenance.
- I. The following policies are applicable to downloaded information:
  - 1. Information downloaded from the Internet or Intranet shall be for City work related purposes only.
  - 2. Downloading of large data images, video, and graphics should be timed so as not to impact the performance of the City network. Very large files should be downloaded after normal business hours.
- J. Internet broadcast services must be approved by the Department Director or designee. Internet broadcast services must utilize the centralized ITD broadcast servers when available.

### 11. Intellectual Property Rights

- A. It is the City of San José's policy to retain all copyrights and other intellectual property rights of which it is the legal owner. All copyrights and other intellectual property rights which are created by City employees in the course and scope of their employment by the City of San José are the exclusive property of the City of San José.

**EXCEPTION:** Works created under the following circumstances are excluded from this policy:

- 1. Works developed entirely by the employee on the employee's own time without using City equipment, supplies, facilities, or trade secret information except for those creations that either:

## Use of E-Mail, Internet Services, and Other Electronic Media

1.7.1

- (a) Relate at the time of conception or production to the City's business, or actual or demonstrably anticipated research or development of the City; or
    - (b) Result from any work performed by the employee for the City.  
For example, an employee may retain rights to artwork, photographs, and writings which are created by the employee at home, which are not related to the employees' work and not intended to be used or purchased by the City of San José.
  2. Copyrights or other intellectual property rights which are created pursuant to an authorized written agreement between the City of San José and the employee which gives a property right to the employee. Agreements shall not be authorized without prior written approval of the City Manager, or designee.
- B. Transfer of Information
1. City employees shall not post material on Internet or Intranet services, send material via e-mail, copy materials, or download materials when such actions would constitute copyright infringement or violation.
  2. Employees shall not transfer or use in the performance of their duties any proprietary or confidential information, whether or not in writing, of a former employer without that employer's written consent.

### 12. Security

- A. City of San José information technology systems shall be protected, operated, and maintained by following the City's Security Standards Handbook as well as the City's [Information and Systems Security Policy](#).
- B. The City reserves the right for any reason to access, disclose and delete all messages and other electronic data sent over its electronic mail system or stored in its files.

### 13. Employee/User Responsibilities

- A. Employees shall not enter or attempt to enter the computer files or e-mail messages of another individual without the employee's authorization or consent, or the consent of the City Manager's Office.
- B. Suspected or identified security violations shall be reported to the Cybersecurity Office. Violators may lose email and/or internet access and may be subject to disciplinary action.
- C. Employees shall not use re-mailing services, or use "anonymous" or "aliases" to protect their individual identities while using City information technology systems or equipment.

**Use of E-Mail, Internet Services,  
and Other Electronic Media****1.7.1**

- D. Employees shall not share their passwords under any circumstance.
- E. All communications should follow proper etiquette, such as:
  - 1. Materials posted by City employees shall professionally represent the City of San José. The transmission of defamatory, obscene, offensive or harassing messages, or messages which disclose personal information without authorization is prohibited.
  - 2. E-mail messages and electronic postings may be read by people beyond the addressee, and upon request may be produced to a court in connection with litigation and should be composed accordingly.
- F. Employees shall not send mass electronic mail messages on a “Department-wide” basis to all Department employees without prior written authorization of the Department Director, or designee. All “City-wide” emails must be approved and sent by the City Manager’s Office.
- G. Employees should carefully consider the names on a mailing list as addressees or copies. Some employees may not want their e-mail addresses to be widely known or to receive responses to widely distributed messages.
- H. Misaddressed e-mail shall be sent back to the original sender with a message that the message has been misaddressed, and the original deleted. However, if the misaddressed electronic mail is offensive, inappropriate or otherwise in violation of this policy, the misaddressed e-mail shall be forwarded to the recipient’s Department Director or designee for appropriate action.
- I. Employees shall not use other e-mail services or third-party e-mail providers, such as Yahoo or Gmail, for City related purposes and shall not use City equipment to access such e-mail for any reason.
- J. Employees shall not use City internet services to access broadcasting of web-streamed music.

Approved:

/s/ Khaled TawfikInformation Technology Department  
Director / Chief Information OfficerSeptember 9, 2025

Date

