

 <b>TECHNOLOGY USE POLICY</b>	<b>Citywide Policy Manual Policy #3.01</b>
	<b>Attachments:</b> N/A
<b>Effective Date:</b> December 3, 2024	<b>Responsible Department:</b> Innovation & Technology
<b>Related Policies &amp; Notes:</b> This policy supersedes the November 2018 Technology Use Policy	

### Purpose

The purpose of this policy is to provide guidance and set forth the acceptable use of City Technology Resources by Computer Users at the City of Cupertino ("City") to ensure technology resources are used in an appropriate, responsible, and lawful manner that protects the City and serves its interests.

### Policy

#### Scope and Applicability

This policy applies to all City employees, elected officials, commissioners, contractors, consultants, temporary workers, interns, volunteers, and vendors ("Users") who are provided access to City Technology Resources.

The policy covers the following topics pertaining to use of City Technology Resources:

- Definitions
- General
- E-Mail
- Internet
- Network and Cybersecurity
- Required Security Awareness Training
- Computer Equipment and Software
- Mobile Devices
- Data and Information
- Telephones and Voicemail
- Technology Purchases
- Separation or Discontinuance of Services
- Netiquette
- Violations

## Definitions

The following definitions apply to this policy.

### a. City Technology Resources

City Technology Resources refers to the City's computing and communications environment and resources used to create, process, store, and transmit data and information, including, but not limited to, the City's network (wired and wireless, including guest Wi-Fi), electronic mail system (e-mail), Internet service, desktop, and laptop computers, systems and applications software, data, storage, mobile electronic devices, including smartphones and tablets, cell phones, telephone system and telephone handsets, voice-mail system, pagers, printers, copiers, facsimile machines, scanners, audio/ video equipment, social media, and cloud-based and third-party software and infrastructure services. This may also be referred to as the City's computing environment or Information Technology systems.

### b. California Public Records Act

The California Public Records Act (CPRA) is a law under California Government Code §6250, et seq., requiring state and local agencies, including the City, to provide access to public (government) records by way of inspection and/or copying to the public upon request unless exempted by law. A public record is a writing prepared, used, owned or retained by a state or local agency pertaining to the conduct of the public's (City's) business, regardless of physical form or characteristic.

SOC1 examples of records that may be exempted from the law include, but are not limited to, the following:

- Files pertaining to data that would constitute an unwarranted invasion of personal privacy if disclosed;
- Pre-decisional, deliberative communications which are not retained in the ordinary course of business;
- Documents pertaining to pending litigation to which the organization is a party;
- Examination data;
- Records exempted or prohibited from disclosure pursuant to federal or state law;
- Employee relations information;
- Attorney-client privileged information; and
- Homeland Security data.

The California Supreme Court held that when a public official or employee uses a personal account and/or device to communicate about the conduct of public business, such as e-mails or text messages, the applicable writings may be subject to disclosure under the California Public Records Act.

Refer to the City Attorney's Office for further guidance on what records require disclosure and to the Clerk of the Council's Office on the process for responding to public records requests.

**c. Confidential Information**

Confidential Data and/or Information is privileged information for a designated purpose that is only intended for recipients with a business need-to-know. Some examples include certain personal information such as medical (e.g.: HIPAA), personally identifiable information (PII), recruitment, disciplinary, and performance information; attorney-client privileged communications; and protected information. Unless exempted by law, some types of confidential information may be subject to legal inspection and/or disclosure requirements.

**d. Contractor/ Vendor**

An independent person or business contracted to perform services for the City.

**e. Copyright**

The exclusive legal rights to copy, reproduce, or sell a specific piece of intellectual property.

**f. Encryption**

Encryption - The coding or scrambling, using sophisticated techniques, of information to prevent third parties from "reading" it.

**g. User**

City employees, elected officials, commissioners, contractors, consultants, temporary workers, interns, volunteers, and vendors who are provided access to the City Technology Resources.

**h. Authorized Approver**

Employees who have been authorized by a Department Head or his/her designee, to make technology requests for their department.

**i. Exempt Employees**

Employees who are not subject to the minimum wage and overtime provisions of the Fair Labor Standards Act.

**j. Mobile Device**

An electronically powered portable device that can view, process, store, and transmit data wirelessly using cellular, radio, satellite, or other communications technology. Examples include smart phones, tablets, laptops, Personal Digital Assistants (PDAs), and cell phones. Also referred to as Mobile Electronic Device.

**k. Personal Mobile Device**

A Mobile Device that is personally owned by a User that is authorized to use City Technology Resources. This can also be referred to as Bring Your Own Device (BYOD).

**l. Mobile Device Management (MOM)**

A system used to administer the management, support, optimization, functionality, and security of mobile wireless devices necessary for the deployment, security, monitoring, and integration within the city computing environment.

**m. Non-exempt Employees**

Employees who are subject to the minimum wage and overtime provisions of the Fair Labor Standards Act.

**n. Intellectual Property**

Refers to a number of types of creations such as books, movies, songs and software. Intellectual property is protected by a body of law collectively referred to as copyright law.



**o. Malware**

Malicious software intending to cause harm and disruption to City Technology Resources. Examples include viruses, worms, Trojan horses, spyware, dishonest adware, and ransomware.

**p. Network**

The collective name for equipment and devices that interchange information using a common medium.

**q. Personally Identifiable Information (PU)**

Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of PU include, but are not limited to:

- Name: full name, maiden name, mother's maiden name or alias
- Personal identification numbers: social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number or credit card number
- Personal address information: street address or email address
- Personal telephone numbers
- Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting
- Biometric data: retina scans, voice signatures, or facial geometry
- Information identifying personally owned property: VIN number or title number
- Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person

## General

### Background

The City utilizes technology resources in every department to support the delivery of public services to City residents, businesses, and the community. Technology is a core element to the effective operation of the City. As such, it is important to have standards in place for its proper use to maximize reliability, integrity, and performance. As with other finite public resources, City staff should be responsible stewards of these resources. These resources should be used judiciously, responsibly, and appropriately.

The City is the custodian of vast amounts of data and records processed and stored in its information systems. In addition to public information, there are considerable amounts of sensitive and confidential data. The City is responsible to protect and safeguard its data and systems from unauthorized access, corruption, and loss.

Technology solutions and deployment models continue to evolve and become increasingly complex. The City's technology environment includes a hybrid of on premise and cloud-based solutions. Many City systems utilize the Internet in some way, and many are integrated and inter-dependent upon one another. Computer operating systems, applications software, and hardware firmware are continually being updated to provide improvements and bug fixes.

Increased Internet connectivity, inherent vulnerabilities in systems, and new malware and cyber-attacks expose City information systems and data to increasing threats.

This Technology Use Policy puts in place rules and expectations for responsible use of City Technology Resources to optimize value, reliability, integrity, and performance of City information systems, comply with laws, reduce risk of loss and exposure, and protect the City, its image, and interests. Users are required to comply with the provisions of this policy.

#### *1.1 No Expectation of Privacy*

City Technology Resources are the property of or placed into service for use by the City. Users have no reasonable expectation of privacy in the use of City Technology Resources.

At any time and without prior notice, the City may monitor and examine e-mail, website access, network and Internet activity, computer files, and other information transmitted through or stored on City Technology Resources.

Logs are recorded for accessing various City Technology Resources such as, but not limited to, network and systems, websites, email, and data / electronic transactions.

Records, regardless of form, pertaining to the conduct of City business are subject to the California Public Records Act (CPRA) and may be publicly disclosed. Records may also be discoverable and disclosed as allowed under law in the event of litigation.

City Technology Resources, such as assigned computers or mobile devices, may be subject to seizure or subpoena in criminal or civil investigations or cases.

### *1.2 Acceptable Use*

City Technology Resources should be used for conducting City business. Examples of allowable use of City Technology Resources include the following:

- To facilitate the performance of job / service functions.
- To facilitate the communication of business-related information.
- To schedule and coordinate meetings with individuals, venues, and City resources.
- To communicate with departments and outside individuals and organizations to perform a job / service function.
- To store and access City documents and data related to City projects and functions.
- For research and education required to perform job / service functions. Incidental personal use of City Technology Resources is acceptable if it does not interfere with the normal performance of a user's work duties or overburden City resources. Personal use should be *de minimis* and without cost or increased risk to the city.

### *1.3 Prohibited Use*

Prohibited use of City Technology Resources include, but are not limited to, the following:

- Illegal activities.
- Making threats, harassment, slander, defamation, promotion of violence or hate.
- Obscene or sexually explicit images or communication.
- Use with malicious intent.
- Intentionally causing disruption, damage, or loss to City Technology Resources.
- Violation of copyright laws.
- Using unlicensed software.
- Installing non-work-related software without approval of I&T.

- Installation of non-City owned hardware or software.
- Utilizing City-owned software for personal use.
- Copying City-owned software and/or data to local devices, e.g. laptop, desktop, and/or mobile device.
- Unauthorized access to networks, systems, services, files, data, e-mail or voicemail.
- Political endorsements, solicitations, or religious promotion.
- Gambling and game playing.
- Personal gain private use, working for another business, or commercial activities.
- Storage of personal music, videos, photos or files.

#### *1.4 Downloading or Opening Internet Files or E-mail Attachments*

Downloading or opening files from the Internet or email attachments expose the City to potential harm from malware. Although City Windows-based computers have anti-virus software installed, this software does not protect from all malware.

1. Users should not download or open files on the Internet unless there is a business purpose.
2. Users should exercise extreme caution when downloading or opening files from the Internet or in e-mail attachments.
3. Users should NOT download or open executable files or attachments. Common executable files have the following extensions (the last 3 letters after the last dot). This is not an exhaustive list.
  - Programs: .exe, .com, .msi, .msp, .cpl, .hta, .jar, .scr, .application
  - Scripts: .bat, .cmd, .vb, .vbe, .vbs, .js, .jse, .ps1, .ps2, .ps1xml, .ps2xml, .ws, .wsf
  - Shortcuts: .scf, .lnk, .inf; Registry: .reg
  - Microsoft Office files that contain macros: .docm, .dotm, .xlsm, .xltm, .pptm
4. Users should not download, or extract compressed or archived files from the Internet or in e-mail attachments without oversight from I&T. Compressed files may have malicious executables within them.

Common compressed file extensions are .zip, .7z, .rar, .r00, .r01, etc.

5. Users should contact I&T if uncertain about downloading or opening a file or e-mail attachment.

### *1.5 Representation*

Use of a City e-mail address or IP address represents the City when communicating with an external party or using an external service, such as a newsgroup, bulletin board, or listserv. Users authorized to interact with external parties or services should conduct themselves professionally and appropriately within the context of their role and/ or authority at the City.

### *1.6 Good Judgement*

Users should use common sense and reasonable judgement when using City Technology Resources.

## **2 E-Mail**

### *2.1 Authorization*

1. New requests must come from an Authorized Approver or Human Resources to obtain a city e-mail account.
2. Non-exempt hourly employees are prohibited from checking or accessing City e-mail during off-duty hours unless pre-approved by the employee's supervisor. Non-exempt employees will be compensated for any approved overtime.

### *2.2 General E-mail Provisions*

1. Users are to use City e-mail accounts when sending messages pertaining to City business.
2. Use of personal e-mail accounts for City business should only be used on an exception basis (e.g.: offsite with no access to City e-mail). In such a case, the User's City e-mail address or an appropriate City e-mail address should be copied (cc'd).
3. E-mail messages sent from City e-mail addresses have the same effect as sending on City letterhead.
4. E-mail messages sent from City e-mail addresses or pertaining to the conduct of City business should be professional and business appropriate.

### *2.3 Disclosure*

1. E-mail messages pertaining to the conduct of City business are subject to the

California Public Records Act (CPRA) and may be publicly disclosed unless exempt by law. This applies to e-mails using City Technology Resources as well as personal e-mail accounts and/or from personal devices.

2. Users are required to provide the city with copies of any e-mail messages in their personal e-mail account(s) and/ or devices that pertain to the conduct of City business that are responsive to a PRA request except as exempt by law.
3. E-mail messages may also be discoverable and disclosed as allowed under law in the event of litigation or a criminal investigation.
4. The City may archive e-mail messages of City e-mail accounts. Archived e-mail messages will be retained per the City's retention policy even if a user deletes messages from their email software client (e.g.: Microsoft Outlook). Archived e-mail messages are subject to PRA except as exempt by law.

#### *2.4 Special E-mail Access Authorization*

1. It may be necessary for a User to access another User's e-mail account under special circumstances. In such a case, the Department Head must authorize access by submitting a written request to I&T.

#### *2.5 Mailbox Storage Size*

1. Users are responsible for managing and controlling the contents and size of their city email mailbox.
2. User e-mail mailbox storage will be limited to a maximum size threshold identified on the city intranet.
3. Warning messages will be sent if the e-mail account maximum storage size is being approached.
4. If the maximum storage size of an e-mail mailbox is reached, the e-mail User will be notified, and e-mail service may be suspended. The service suspension will continue until the e-mail account storage size has been reduced below the maximum size threshold.
5. Users who have a justifiable business requirement for mailbox storage size in excess of the city maximum may submit a Request for Increase to their Department Head and the Innovation Technology Director.

## 2.6 *E-mail Retention*

### 1. Purpose of E-mail System.

The City's e-mail system is a communications system and is not intended to be used as a records storage system. E-mail messages are generally transitory communications not retained in the normal course of business.

### 2. Retaining E-mail Business Records.

To the extent that e-mail messages constitute official business records to be retained pursuant to the City's records retention policy, such e-mail messages shall be retained using one of the following methods.

- a. Move messages out of Inbox or Sent Items folders to another e-mail folder.
- b. Save the message or output it to a PDF electronic file and store in an official electronic records storage repository.

Users are responsible to follow the City's records destruction procedure for retained email messages that are official business records when the records retention requirement has been met.

### 3. Retaining E-mail Pertaining to Litigation.

E-mail messages pertaining to an anticipated or actual legal action must be retained until the litigation is concluded regardless of the records retention requirements. City Attorney, Administrative Services Director and Innovation Technology Director should be notified of such E-Mail messages

### 4. Deleting E-Mail Messages.

E-mail messages that do not serve a business purpose shall be routinely discarded. For that reason, each user has the same responsibility for their e-mail messages as they do for any document they obtain in the course of their official duties and must decide which communications should be retained for business or legal reasons and which should be discarded. If a user has any questions regarding whether an e-mail should be retained as a business record, he or she should seek guidance from their supervisor and/or Department Head who may consult with the City Attorney's Office as necessary.

### 5. Automatic Deletion of Messages in Inbox, Sent Items, and Deleted Items Folders.

E-mail messages in users' Inbox, Sent Items, and Deleted Items folders will be automatically deleted based on defined rules as early as 90 days from receipt or generation. If a message constitutes an official business record that requires being retained pursuant to the City's records retention policy, the user should preserve the message as described above within 90 days.

6. Local E-Mail Archives Not Supported.

The use or creation of local e-mail personal archive files (e.g.: Outlook.pst files) are not supported. Such archive files are not backed up. Users shall not store official business records in such files.

7. E-mail System Backups.

The City's e-mail system is backed up to separate media regularly and stored offsite for disaster recovery purposes. Backups are not retained for the purpose of archiving messages for future retrieval.

### 3 Internet

Access to the Internet exposes the City to external threats to its information systems and data. As such, the City takes precautions to protect itself from these threats using cyber-security systems and controlling and managing Internet access.

#### 3.1 Internet Services Provided

The following Internet services are provided to authorize Users.

- E-mail. Send/ receive E-mail messages to/ from external recipients/ senders.
- Web Browsing. World-Wide-Web (WWW) services using the hypertext transfer protocol (HTTP or HTTPS - Secured) through web browser software (e.g.: Internet Explorer or Google Chrome).

The following Internet services are only allowed on an as-needed basis with business justification and I&T approval.

- File Transfer Protocol (FTP, SFTP or FTPS - Secured). Send/ receive files over the Internet to/ from an FTP server. Business use examples include mandatory data reporting to the State or authorized data interchange with a business partner (e.g.: bank or service provider).
- Software as a Service (SaaS) applications. Allows the connection to City applications housed on the Internet.
- Peer to Peer File Sharing (P2P). Peer to Peer file sharing allows one to download or upload files with others (nodes) on the Internet typically using torrents and P2P software. This service is not typically used for business purposes and is strictly prohibited without a compelling business case.



### 3.2 *Prohibited Websites*

Intentional access to websites that promote or predominantly contain the following content are prohibited:

- Obscene or Sexually Explicit Content
- Illegal Activities
- Violence or Hate
- Online Gambling and Gaming

The City maintains the right to enable website content monitoring and filtering software that will block prohibited website access and monitor user browsing history. Regardless of website filtering is in place, Users should take care to not intentionally visit prohibited websites.

## 4 **Network and Cybersecurity**

### 4.1 *Network Access*

The City's computing environment is comprised of a common network that includes a collection of cabling, switches, routers, gateways, access points, servers, operating systems, databases, applications, and other technology resources. Access to the City computing environment is by way of a network user account (AKA network domain account or Active Directory (AD) account).

Users must receive authorization from their supervisor, Department Head or their designee, or sponsoring Department contact and Human Resources to obtain a City network user account. The Human Resource contact must submit a Network Access Request to I&T and specify the requested network services.

I&T may revoke access to City Technology Resources without advance notice as required to ensure the security and integrity of the City's network and computing environment.

### 4.2 *Passwords*

User accounts and passwords are used to secure access to network and computing resources. Passwords are the front line of protection for user accounts. A compromised user account can put City Technology Resources at risk and as such, the following rules and terms apply to User passwords.

#### 4.2.1 *Password Rules*

1. Users shall use strong password(s) to access City Technology Resources. Unless other password rules exist for a given system, the following rules should be used when selecting a password.
  - At least twelve characters long
  - Contain a mixture of at least 2 of the following character types: lower case letter, upper letters, and numbers.
  - Must not contain the Username
2. It is suggested that passwords be created that can be easily remembered yet hard to guess. One way to do this is to create a password based on a song title, affirmation, or phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be something like "TmBlw2R!" or another variation.
3. Network User account passwords will expire at a set time interval (e.g.: 6 months). A Windows message will indicate pending password expiration when the expiration date is approaching and will provide a link to reset the password.
4. The last 5 passwords cannot be used when resetting a network User account password.
5. Network User accounts will become locked after 5 failed attempts with the wrong password. Contact the I&T Help Desk in the event of a locked account.

#### 4.2.2 *Password Protection*

User account passwords are to be treated as sensitive and confidential.

1. Users are not to share passwords with anyone. This includes supervisors, administrative assistants, authorized users, unauthorized users and I&T support personnel.
2. User passwords should not be written down.
3. Passwords should not be sent in an e-mail, text message, or voice mail.
4. If a file is used to store passwords, the file should be encrypted and a strong password used.
5. Users who suspect their account or password has been compromised should change their password immediately and report the incident to their supervisor and I&T.

6. Accounts are to be used only by the assigned authorized user of the account. Attempting to obtain another user's account password is prohibited.
7. Users should lock their computer (on Windows computers, while holding down <Ctrl> & <Alt> keys, press <Delete> key, click Lock), log-off, or shut down their computer when not in use.

#### 4.3 *Muti-Factor Authentication*

MFA is mandatory for all users accessing the City's network and applications. This applies regardless of the user's location, or the device being used. MFA adds an additional layer of security by requiring users to provide two or more verification factors to gain access, thereby reducing the risk of unauthorized access.

#### 4.4 *Remote Access*

##### 4.4.1 *Authorization*

1. Remote access to the City's network over the Internet (Virtual Private Network - VPN) will be considered based on business-need on a case-by-case basis. A request for remote access must be authorized by the User's Department Head or City Manager or their designee. The following general criteria will apply to who may be considered.
  - a. The employee's job responsibilities can be effectively performed outside the office without compromising productivity or quality of work.
  - b. Tasks do not require daily physical presence, such as in-person customer service, handling physical documents, or operating specialized equipment located at the office. City employees approved for the City's telecommute program.
  - c. City employees under special circumstances.
  - d. Contractors, consultants, and vendors providing services to the City such as I&T support.
2. Non-exempt hourly employees are prohibited from accessing the City network and systems during off-duty hours unless pre-approved by the employee's supervisor. Non-exempt employees will be compensated for any approved overtime.
3. Information about the User's remote computing environment must be provided to Human Resources as part of the remote access request. I&T will review and assess the information to assess the security risk for consideration in granting remote access.

#### 4.4.2 *Other Provisions*

1. Aside from City-provided computer, software and mobile devices, the remote User is responsible for providing, configure, and support Internet access.
2. Remote Users shall not provide access to or to share City data or printed reports to others except as authorized by their supervisor or assigned City contact. Remote Users shall protect City systems access, data, and printed reports from unauthorized access or disclosure. Proper protective measures include securing the remote computer and reports when unattended and shielding remote computer and reports from unauthorized viewing. Reports containing sensitive or confidential data should be shredded or obliterated prior to disposal.
3. Remote User sessions will be automatically disconnected after a designated threshold of time of inactivity. The User must then log on again to reconnect to the network.
4. Split tunneling is not permitted. Users are not allowed to connect to any other network, including their own private network, while remotely connected to the City network. However, local LAN connections for Internet access only are permitted, ensuring that all other traffic is routed through the City network for security purposes.
5. Department supervisors or assigned Department contacts shall immediately notify I&T when the need for a User's remote access has ended.

#### 4.5 *Anti-Virus*

I&T will install and configure anti-virus/ malware software on City-issued computers and network devices. Anti-virus / malware software detects and prevents most viruses and malware from causing harm, but it is not perfect. New malware comes out often which constantly poses new threats.

Users are to not interfere with the anti-virus/ malware software installed on their assigned computer.

Users authorized to use their own computers or mobile devices for City business must be sure their equipment is on a supported operating system and include reputable anti-virus/ malware software with up-to-date anti-virus/ malware definitions. Users are to immediately contact I&T if they suspect their computer has been infected by a virus or malware. It is advised to immediately disconnect the computer from the network if possible.

#### *4.6 Required Security Awareness Training*

Given the sensitive nature of the information that municipalities handle (e.g., resident data, financial records, personally identifiable information, etc.), it is critical that employees and elected officials are educated on the latest cybersecurity threats and how to prevent them.

##### *4.6.1 Reasons for Requiring Security Awareness Training:*

- a. **Protection of Sensitive Data:** Local governments store and process confidential information, such as personal identification details, social security numbers, and payment data. A security breach can expose this data, leading to identity theft, financial losses, and reputational damage.
- b. **Increased Cyber Threats:** Governments are increasingly targeted by cybercriminals through phishing attacks, ransomware, and social engineering due to the value of their data and critical infrastructure. Training helps staff recognize and respond to these threats.
- c. **Human Error Mitigation:** Human error is one of the leading causes of data breaches. Proper training ensures that employees are aware of best practices, reducing the risk of unintentional mistakes that could lead to a cyber incident.

##### *4.6.2 Consequences if Staff Do Not Complete the Training:*

- a. **Increased Vulnerability to Attacks:**
  - Untrained staff are more likely to fall for phishing scams, inadvertently download malware, or expose systems to cyber threats, potentially leading to data breaches.
- b. **Financial Losses:**
  - Data breaches can result in significant financial costs, including remediation expenses, fines for non-compliance, and potential lawsuits. Governments may also face increased cybersecurity insurance premiums.
- c. **Operational Disruption:**
  - Ransomware attacks can cripple local government operations, delaying public services and eroding trust among residents. In some cases, it can take weeks or even months to fully recover.
- d. **Legal and Compliance Issues:**
  - Failing to ensure staff complete mandatory training can result in non-compliance with regulatory standards, leading to penalties or sanctions from oversight bodies.

e. Reputation Damage:

- A breach caused by staff negligence can severely damage the public's trust in their local government's ability to protect sensitive information.

#### 4.6.3 Required Training

- Onboarding Requirement: Completion of initial security awareness training is a condition of employment for all new hires, including elected officials.
- Annual Refresher Requirement: Completion of annual security awareness training is a condition of employment for all staff, including elected officials. This must be completed in a month's time of being issued.
- Phishing Simulations: Conduct regular simulated phishing exercises to assess employee responses. Employees who fall for simulated attacks are required to complete additional training in a month's time.

#### 4.6.4 Consequences for Non-Compliance

a. First Reminder (Friendly Notification):

- Send an email reminder one week before the deadline and again on the due date. Emphasize the importance of completing the training to protect City resources.

b. Second Reminder (Formal Notification):

- If the deadline is missed, a more formal notice to the employee, cc'ing their Department Head. Include a new deadline (e.g., 5 business days) to complete the training.

c. Disciplinary Action:

- If the training deadline is missed, the situation may be escalated to Human Resources for disciplinary action up to and including termination.

## 5 Computer Equipment and Software

I&T will assign computer equipment and software to employee Users necessary to perform their job functions. The City may provide computer equipment and/ or software to other classification of Users who provide services to the City (i.e.: volunteers, contractors or vendors) as approved by the sponsoring User's Department Head or his or her designee and the I&T Director or his or her designee.

### *5.1 Computer Equipment*

Computer equipment includes items such as, but not limited to, personal computers (also referred to as desktop computers or workstations), laptops, storage, monitors, docking devices, keyboards, mice, printers, plotters, scanners, speakers, cameras, and cables.

1. Users are responsible to protect and properly care for their assigned computer equipment.
2. Users shall use City computer equipment properly and not misuse it. Users should contact I&T if they need assistance on using computer equipment.
3. Users should not use computer equipment assigned to another without the User's supervisor's permission.
4. Users should always use their own network user account to login, even when using another User's computer.
5. City-owned computer equipment may only be procured, installed, changed, or removed by I&T unless approved by I&T.
6. I&T will coordinate the disposal of computer equipment. Computer equipment may have special disposal requirements and may contain confidential information that needs to be properly wiped.
7. Additional provisions for laptops, tablets, and smartphones are in the Mobile Devices section.

### *5.2 Software*

Software includes, but is not limited to, operating systems (e.g.: Microsoft Windows), Microsoft Office (e.g.: Word, Excel, PowerPoint, Access), applications, anti-virus and other utility software.

1. Software installed on or used through City Technology Resources must be approved by I&T. This includes client application software (sometimes referred to as "thick" or "fat" client software) or Software as a Service (SaaS), also referred to as cloud-based application services.
2. All software used by Users on or through City Technology Resources must be licensed or the City must have legal right to use (e.g.: in-house developed).
3. Unauthorized use, copying, transfer, or reproduction of licensed software is prohibited and in violation of copyright laws. Copyright infringement can subject

the User and City to liability for damages to the software manufacturer. I&T will maintain an inventory of City-owned software licenses.

4. Software may only be procured, installed, changed, or removed on City Technology Resources by I&T staff unless otherwise approved by I&T.
5. Users are not permitted to interfere with anti-virus or anti-malware software installed on their assigned computer(s).

## **6 Mobile Devices**

### *6.1 Authorization*

Users must receive authorization by their Department Head or his or her designee in order to access City Technology Resources using a mobile electronic device ("Mobile Device").

Additionally, mobile devices must be approved to access City Technology Resources by the Innovation and Technology Department (I&T). Refer to I&T for a list of approved mobile devices.

### *6.2 Personal Mobile Devices*

Users who have been authorized for mobile access to City Technology Resources may request to use their personal mobile device. The User's Department Head and I&T may authorize this. The following understanding and terms apply to using a personal mobile device for City business use.

1. The City does not expect or require employees to provide a personal cell phone to perform any of the employee's assigned job duties. If the Department Head determines a mobile device is required to perform one's job duties, he or she will authorize the issuance of a City-owned mobile device or provide a monthly stipend to reimburse the employee for monthly fees when the phone is used for City business purpose. The reimbursement rate is as follows:

- Up to \$55 per month (basic City rate plus taxes) for smart phones

Cell phone stipends are not considered an "allowance" for employees, in which an employee would receive a flat amount. Rather, employees will be reimbursed for an amount up to \$55/month for smart phones. Calculation for reimbursement is as follows:

- $\text{Main line charge} + (\text{total data} + \text{total tax} + \text{total fees}) / \text{total\# of lines}$
2. The City may prohibit an employee from using his or her personal device to conduct City business at any time, with or without cause.



3. Non-exempt hourly employees are prohibited from using their personal devices for City-business during off-duty hours unless pre-approved by the employee's supervisor. Non-exempt employees will be compensated for any approved overtime.
4. The use of personal devices to access City Technology Resources shall be subject to the technology controls, policies, and security that are provided and implemented for City- owned devices unless stated otherwise herein.
5. Users have no reasonable expectation of privacy while using City Technology Resources from their personal mobile device such as network traffic, website access, and e-mail messages. To the extent that Users wish their private activities remain private, they should not access City Technology Resources from their personal device.
6. Users provided a monthly stipend for the use of their personal device are responsible for all costs in excess of the monthly stipend including, but not limited to, the cost of the device, service plan, accessories, maintenance, repair, and any insurance or warranties.
7. The City is not responsible for damage to users' personal devices including when being used for City business and accessing City Technology Resources.
8. A user is responsible for all activity performed from his or her mobile device when using the City's Technology Resources and will take all reasonable care to protect his/her device from unauthorized access, compromise, and to be free from malware.

### *6.3 Mobile Device Management*

City-owned mobile electronic devices will be centrally managed by I&T and use the City's Mobile Device Management (MDM) system to help manage mobile device inventory, software, policies, and security.

1. All authorized mobile devices shall only be managed and supported by authorized I&T staff.
2. Users shall not attempt to bypass mobile security and management.
3. Authorized Users shall maintain data on a mobile electronic device in accordance with the City's Records Retention and Destruction Policy.
4. City information on City-owned and personal mobile electronic devices may be subject to the California Public Records Act, the Brown Act, or any other California laws pertaining to public employees/officials. Users must comply with public

records request related to City data on City or personal mobile electronic devices.

5. Any approved personal mobile device (non-City issued) that is connected to the City's computing environment must comply with the standards in this policy.
6. I&T may activate audit trails without notice for the purpose of identifying unusual usage patterns or suspicious activity to determine if the mobile device has been compromised or to identify misuse.
7. The City reserves the right to audit the configuration and content and inspect files stored on City-owned mobile devices without notice.

#### *6.4 Mobile Device Security*

All mobile electronic devices shall be physically and electronically protected at all times. This includes, but is not limited to the following:

##### Physical Security (City-owned Devices)

1. Smart Phones should be equipped with a case to reduce risk of physical damage during a drop.
2. Mobile devices should not be left unattended in any public locations.
3. Mobile electronic devices shall not be left in vehicles in plain sight.
4. Physical security such as a laptop cable lock or a locked cabinet should be used when left unattended in work areas.

##### Electronic Security

1. Users shall protect access to their mobile device with a strong password, PIN, or bio-metric (e.g.: facial recognition) security.
2. Users shall not disclose their passwords or PIN's to others.
3. Users shall not tamper with anti-virus or anti-malware software installed by I&T on any client computers.
4. Users will not modify City-owned mobile devices without approval of I&T.
5. I&T may restrict the mobile device or User from accessing certain City Technology Resources.
6. The User shall not store City data to resources outside the City computing environment, such as local desktop/laptop/tablet storage, Apple iCloud, Dropbox, Google Drive, Microsoft OneDrive, or other cloud-based file storage services without approval from I&T.

7. Users should not use City-owned devices as Hotspots without approval by I&T.
8. I&T may remotely disable, wipe (erase), or reset City-owned mobile devices under the following circumstances:
  - a. Device is lost or stolen.
  - b. Device is replaced by another device or retired without replacement.
  - c. Device is transferred to another User.
  - d. User separates from the City (e.g. retirement, resignation, termination).
  - e. To repair a software issue (with knowledge of the User).
  - f. The device is infected by a virus or other malware.
  - g. To protect City Technology Resources.
  - h. Upon request of the User's Department Head or his or her designee.

#### 6.5 *Mobile Device Data*

1. Access to City data/information shall be provided on a "need-to know" basis and with security rules in place to protect from unauthorized access.
2. Wherever possible, data is to reside on the City's network rather than downloaded to the device.
3. Sensitive and Confidential Data

Access to sensitive and/or confidential data on mobile devices must be made securely and with considerable care.

  - a. Encryption should be used.
  - b. City data should not be stored on mobile devices.
4. Any City business electronic communication, or information stored on a mobile device, City-owned or personal, may constitute a record subject to disclosure under the California Public Records Act (CPRA), the California Code of Civil Procedure, the Federal Rules of Civil Procedure, or other applicable statutes, regulations, or legal authorities. Users shall provide access and/ or produce records that meet the requirements for public disclosure stored on the mobile device upon the City's request.
5. Authorized Users and mobile devices may connect to the City's e-mail services. Other City services may be provided as authorized.
6. It is the User's responsibility to back-up any incidental personal data and

applications on City-owned devices. In the event the device needs to be-wiped, all data and applications will be lost. The City bears no legal or financial responsibility for loss to personal data or applications.

#### 6.6 *Lost or Stolen Mobile Devices*

Users shall promptly report lost or stolen mobile devices to I&T within 24 hours or as soon as reasonably possible. City-owned devices will be remotely wiped and locked to prevent unauthorized access. If the device is recovered, it can be provided to I&T and re-provisioned. The user's City network password should be changed as soon as possible after the device is lost or stolen.

#### 6.7 *Mobile Device Support*

##### 1. City-Owned Mobile Devices

- a. City-owned mobile devices are supported by I&T during I&T Help Desk hours.
- b. Requests for new mobile devices or support should be submitted to the I&T by e-mail at [helpdesk@cupertino.org](mailto:helpdesk@cupertino.org), or by calling 777- (City Hall) or 714-245-8411 (PD).
- c. Departments are responsible for paying monthly data and/or voice plans. In the event data or minutes exceed the monthly plan the employee is responsible to pay for all personal use minutes or data utilized that exceed the plan limits.
- d. Users should not attempt to repair City-owned devices themselves. Contact I&T for assistance.
- e. I&T will make best-effort attempts to fix problems Users experience on their mobile device. However, it may become necessary to reset a device to factory settings or wipe it to clear a problem. In such a case, I&T will re-initialize the device for City business use. The City is not responsible for personal data or applications lost. The User will be responsible for restoring any incidental personal data and applications.
- f. Mobile applications required to conduct City business must be approved by I&T prior to installation.
- g. Applications should be updated by downloading updates when prompted. It is recommended that mobile applications be updated to keep them

running properly.

- h. I&T pays for mobile device repairs and / or replacements. In the event that abuse or severe negligence resulted in damage the employee may be held responsible for repair costs.

## 2. Personal Mobile Devices

- a. Authorized Users may use supported personal mobile devices for accessing City e-mail and other authorized City Technology Resources.
- b. I&T will assist in configuring the device's City e-mail, remote access, and other City Technology Resources as authorized on the personal mobile device.
- c. The User is responsible for their own device and application support from the manufacturer or third-party.

## 7 Data and Information

### 7.1 Access and Disclosure

- 1. Users may have access to data and information ("Data") in City information technology systems through their system user account(s) and in the course of performing their job duties or service functions.
- 2. Regardless of system access capability, Users shall not search or seek out Data in City systems, databases, repositories, and files except as necessary in the performance of their job duties or service functions.
- 3. Users shall not share or disclose Data in City systems, databases, repositories, and files to others except as necessary in the performance of the User's job duties or service functions.
- 4. Any disclosure should be in compliance with departmental policies and procedures and local, state, and federal laws.
- 5. Users should consult with their supervisor to obtain guidance if uncertain about sharing or disclosing Data.

#### 7.1.1 Sensitive and Confidential Data and Information

- 1. Confidential Information is privileged information for a designated purpose that is only intended for recipients with a business need-to-know.
- 2. Disclosure of confidential data may violate local, state, and/or federal laws.

3. Users shall not access, take, copy, share or disclose sensitive and/or confidential Data without the authorization from their Department Head or his or her designee.

## *7.2 Data Storage and Backups*

### *7.2.1 File Storage*

Files should not be stored on User workstations, portable or mobile devices. These systems and devices are not backed up, and the information may be lost.

City information technology systems store Data on servers used to conduct City business. Data stored on production City-maintained servers are backed up nightly.

Users should store Data pertaining to City business on production City-maintained servers.

### *7.2.2 Sensitive and Confidential Data*

1. Users shall not store or copy sensitive and/or confidential information on external storage systems including removable media (e.g.: USB / Flash drives, SD memory cards, CD/DVDs) or cloud-based services (e.g.: Google Drive, iCloud, One Drive, Drop Box), unless authorized by the I&T Director. Executive Director of Information Technology or his or her designee. If removable media is used, the device must be encrypted and password-protected. If removable media is lost or stolen, the loss should be reported immediately to I&T.
2. When a storage device containing sensitive and/or confidential information needs to be disposed of (e.g.: retention expiration, retirement of hardware, no longer needed, etc.), it should be provided to I&T for proper disposal. The disposal will involve the media be over-written at least three times using specialized software designed to permanently erase data, physical destruction (e.g.: crushing, shredding, incineration), or degaussing (magnetic destruction).

## *7.3 Data and Records Retention*

### *7.3.1 Retention and Destruction*

City records are subject to the City's Records Retention and Destruction Schedule. This schedule serves as policy for retaining and destroying City records. Users shall adhere to and comply with the Records Retention and Destruction Schedule. Records are not to be destroyed without proper authorization and following the records destruction process required by the Clerk of the Council's and City Attorney's Offices.

### 7.3.2 Pending Litigation

California Assembly Bill 5 (Electronic Discovery Act) requires processes and technologies to be in place related to finding and managing electronically stored information that might be relevant in a foreseeable legal dispute. The law requires the agency to stop any automated or regular purging of relevant electronically stored information at the first notification that a legal dispute may be forthcoming. Users are to suspend any record and information destruction plans for any records or information that may be related to a pending litigation. Users should contact the City Attorney's Office for guidance in such circumstances.

## 8 Telephones and Voicemail

Telephones and voicemail are provided at City offices and assigned to Users for the purpose of conducting City business communication. Users shall be professional and responsible when using the City's telephone and voicemail systems.

Telephone calls are logged and may be reviewed by supervisors and/or City management. Provisions for use of mobile phones or smart phones are identified in the Mobile Devices section of this policy.

## 9 Technology Purchases

Centralized information technology standards, architecture, processes and practices maximize the reliability, integrity, efficiency and performance of City Technology Resources. As such, I&T is responsible for all technology-related purchases or contracts.

Departments should contact I&T prior to purchasing or entering into an agreement for information technology goods, services, or support. For large projects, I&T should be contacted early in the planning process.

Users request computer hardware or software through the I&T Help Desk. I&T will review and approve or reject purchase requests based on standards, strategic direction, available resources, and ability to support.

The technology equipment that is being replaced must be turned over to I&T upon replacement. Replaced equipment may be redistributed or reallocated to other users.

I&T will maintain an I&T asset inventory database.

## **10 Separation or Discontinuance of Service**

The following provisions apply to Users who separate or discontinue service from the City:

1. The User shall return his or her City-assigned Technology and other Resources (e.g.: mobile devices, parking and building access cards) to his or her supervisor or assigned City contact before leaving the City. The User's supervisor shall then turn the City Technology Resource(s) in to I&T or make a request to re-provision the Resource(s) to another User.
2. The User should forward any e-mails pertaining to the conduct of City business sent from their personal e-mail account(s) to their supervisor or assigned City contact e-mail address.
3. The User's network and system accounts will be disabled after the separation date. Human Resources will provide I&T the date/time user accounts should be disabled.
4. The User should not attempt to access City Technology Resources even if resources appear accessible.

## **11 Netiquette**

Users are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to, the following:

1. Be Polite. Never send, or encourage others to send, abusive messages or communications
2. Use Appropriate Language. Users are representatives of the City. A User may be alone with their computer, but what is written online or in e-mail can possibly be viewed publicly. Users should never swear, use vulgarities, or any other inappropriate language online or in e-mail.
3. Privacy. Users should not reveal personal data online or in e-mail (e.g., home address, telephone number, etc.).
4. Disruptions. Users should not use City Technology Resources in a way that would disrupt or disturb others. Do not use computer sound or use a low volume when working near others. Silence mobile phones during meetings.
5. Be Brief and Concise. Long extraneous communication is not as effective.
6. Proofread and Spell Check. It is a good idea to proof-read and spell-check messages before sending. Try to make communication easy to understand and to read.



7. Appropriate Message Distribution. Users should send and copy (cc) messages to appropriate recipients. Avoid unnecessary or inappropriate distribution.
8. Consider that humor and satire are very often misinterpreted and can be unprofessional.
9. Cite references for any facts presented.
10. Forgive the spelling and grammar errors of others.
11. All Users are human beings. Don't "attack" correspondents; persuade with facts.

## 12 Violations

Violations of the City's Technology Use Policy may result in removal of access to City Technology Resources and/or be subject to disciplinary action, up to and including termination. In the case of illegal activity and/or malicious use, the City may refer the violation to law enforcement and/or the City Attorney for potential criminal investigation and prosecution and/or civil action.

<p>City Manager's signature: <u><i>Pamela Wu</i></u></p> <p>Date: <u>12/03/2024</u></p>
---

**Revisions: 11/2018**






# Technology Use Policy

Final Audit Report

2024-12-04

Created:	2024-12-04
By:	Janet Liang (janetl@cupertino.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAZsz9zMC_H8iWfE_uFQhe2UVs_bhq__Bc

## "Technology Use Policy" History

-  Document created by Janet Liang (janetl@cupertino.org)  
2024-12-04 - 0:10:36 AM GMT- IP address: 24.6.211.237
-  Document emailed to Pamela Wu (pamelaw@cupertino.org) for signature  
2024-12-04 - 1:04:04 AM GMT
-  Email viewed by Pamela Wu (pamelaw@cupertino.org)  
2024-12-04 - 1:05:56 AM GMT- IP address: 52.202.236.132
-  Document e-signed by Pamela Wu (pamelaw@cupertino.org)  
Signature Date: 2024-12-04 - 3:49:38 AM GMT - Time Source: server- IP address: 64.165.34.3
-  Agreement completed.  
2024-12-04 - 3:49:38 AM GMT



**CUPERTINO**

## TECHNOLOGY USE POLICY

I have received a copy of the City of Cupertino's TECHNOLOGY USE Policy and have carefully read the policy. I understand that I have had the opportunity to ask any questions concerning the policy and they have been answered completely. By signing below, I acknowledge my understanding and agree to comply with the City of Cupertino's City TECHNOLOGY USE Policy.

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Department