City of Santa Clarita

POLICY/PROCEDURE

Number III-13.4	SUBJECT: USE OF ELECTRONIC COMMUNICATIONS SYSTEMS	
ORIGINAL ISSUE	EFFECTIVE: 11/01/1998	CATEGORY: HUMAN RESOURCES
CURRENT ISSUE	EFFECTIVE: 10/13/2020	SUPERSEDES: III-13.3
RESPONSIBLE DEPARTMENT: CITY MANAGER'S OFFICE		

STANDARD MANAGEMENT PROCEDURE

I. PURPOSE

The City of Santa Clarita provides its employees with technology to conduct the City's official business. In this regard, the City has installed, at substantial cost, equipment such as computers and advanced technological systems such as electronic mail (e-mail) for use to conduct its official business. This policy was created to advise all users regarding the access to and the disclosure of information created, transmitted, received and stored via the use of land-line telephones, City-owned cellular phones, the Internet, City e-mail, computer systems, network infrastructure, and Electronic Storage Systems. This policy also identifies the appropriate use of City cellular phones, ownership of City cellular phones, and addresses privacy of any data contained on or transmitted using City cellular phones, as outlined under this policy.

The City's Policy regarding the use of the Electronic Communications Systems, including, but not limited to, Internet, intranet, telecommuting, and e-mail is, among other things, intended to guide you on the performance of your duties as a City employee. This policy is also intended to place all users on notice that they should have no expectation of privacy when using any of the City's Electronic Communications Systems.

The City reserves the right to monitor Internet use, all e-mail and other computer transmissions, land-line telephones, City-owned cellular phones, as well as any stored information, created or received by City employees within any of the City's Electronic Communications Systems. The reservation of this right is to ensure that public resources are not being wasted and to ensure that the City's Electronic Communications Systems are operating as efficiently as possible in order to protect the public interest. All computer applications, programs, and any information, whether work-related or personal, created or stored by employees on any City information system are City Property.

This Policy addresses general City-wide Internet policies, specific issues related to appropriate content and use of departmental pages, and employee use of Internet and e-mail. All departments and employees are required to follow these general policies and guidelines. The law and associated policy regarding the use of Internet, e-mail, and voice mail are continually evolving.

No person shall access the City's Electronic Communications Systems without reading and complying with the procedures set forth in this Policy.

II. DEFINITIONS

A. **Anti-Virus Software:** A software that helps protect a computer, phone, or other electronic device against malware, viruses, and cybercriminals. Anti-virus software includes programs that look at data — web pages, files, software, applications — traveling over individual computers, computer systems, and the public Internet. It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior. It seeks to block or remove malware and viruses as quickly as possible.

B. **Cell Phone**: A type of short-wave analog or digital telecommunication in which a subscriber has a wireless connection from a mobile telephone to a relatively nearby transmitter. Cell Phone is differentiated from a Smartphone in that the latter has data services enabled to allow more features above and beyond simple voice communication.

C. **Mobile Device:** A **mobile device** is a general term to describe a portable computing device, typically handheld and having a display screen with touch input and/or a small keyboard. Most handheld devices are equipped with Wi-Fi, Bluetooth, NFC, and GPS capabilities that can allow connections to the Internet and other devices. Mobile Devices include cell phones, smartphones, laptops, and tablets.

D. **Electronic Communications**: Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photoelectric, or photo optical system, including but not limited to telephone calls, cellular phone calls, fax machine transmissions, and e-mail.

E. **Electronic Communications Systems**: All electronic equipment, devices, software, data, and/or other means of electronic communication furnished by the City including, but not limited to computer hardware and software; telephones; fax machines; cellular telephones; e-mail; Internet; voice mail; any wire, radio, electromagnetic, photo optical, and photo electronic facilities for the transmission of Electronic Communications; and any computer facilities or related electronic equipment for the Electronic Storage of such communications as well as any newly created devices yet to be created.

F. **Electronic Mail (E-mail)**: E-mail may include non-interactive communication of text, data, images, or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "e-mail", "facsimile" or "instant messaging" system; or voice messages transmitted and stored for later retrieval from a computer system.

G. **Electronic Storage Systems**: Any stored data on any local or network attached media, wire or Electronic Communication incidental to electronic transmission thereof. It also means any stored communications by an Electronic Communications service for purposes of backup protection of such communication.

H. **Handsfree**: An adjective used to describe a device that can be used without the use of hands; most commonly used with mobile phones. Handsfree devices are equipped with both a speaker and a microphone. Common examples of handsfree devices are mobile headsets and earpieces, which can be wired or wireless, as well as blue-tooth devices, which use wireless technology to exchange data over short distances.

I. **Messaging (Instant / Text (SMS))**: A text-based conference over telecommunication lines such as the Internet and/or cellular frequencies between two or more people who may or may be connected at the same time.

J. **Internet**: A worldwide network of networks, connecting informational networks communicating through a common communications language or "protocol."

K. **Land-line**: Standard telephone and data communications systems that use in-ground and telephone pole cables in contrast to wireless cellular and satellite services.

L. **Litigation Hold:** Also known as legal hold, is used to preserve mailbox items for discovery before and during legal proceedings, investigations, or similar events. The goal is to preserve mailbox items from inadvertent or purposeful modification or deletion by the mailbox owner or any user with mailbox access, as well as automated deletion processes. Items in litigation hold are returned when discovery searches are performed.

M. **Retention Schedule:** The City Council approves a resolution establishing the protocol and schedule for retaining information for operational or regulatory compliance needs.

N. **Smartphone**: A cellular phone that is characterized as a wireless telephone set with special computer-enabled features, such as e-mail, text-messaging, Internet, web browsing, fax, and LAN connectivity that provides computing and information storage and retrieval capabilities for personal or business use. Examples include iPhone, and other data-enabled devices running software such as Windows Mobile and Android.

O. **Social Networking Sites**: Any web-based URL site that allows for the public or private posting of messages, photos or video, other than the City's internal intranet (rNet). Social networking sites include, but are not limited to, Facebook, LinkedIn, Instagram, Snapchat, Periscope, and Twitter.

P. **Standards**: Departmental directions or instructions describing how to achieve policy.

Q. **Tablets**: A wireless, portable personal computer with a touchscreen interface. The tablet form factor is typically smaller than a notebook computer, but larger than a smartphone. Examples of a tablet include the Apple iPad.

R. **Telecommuting:** When a City employee performs their job from outside a City facility, using personal or City-issued equipment and communications, to remotely access the City's Electronic Communications Systems.

S. **Users**: Any person approved to use the City's Electronic Communications Systems.

T. **Vendors**: Any private person or business enterprise doing business with the City.

III. POLICY AND PROCEDURES

A. Access of Electronic Communications Systems:

1. No regular, probationary, temporary, seasonal, City employee, volunteer, or vendor or contractor shall access the City's Electronic Communications Systems without reading and complying with the procedures set forth in this Policy.

2. All employees, Councilmembers, Commissioners, vendors and contractors, and volunteers requesting authorization to access the City's Electronic Communications Systems, Electronic Communications, and Electronic Storage shall be given a copy of this and all related technology policies and shall sign an acknowledgement of the policies recognizing the parameters for compliance.

3. All new employees, Councilmembers, Commissioners, vendors and contractors, and volunteers requesting authorization to access the City's Electronic Communications Systems, Electronic Communications, and Electronic Storage must be approved by their immediate Supervisor and Technology Services.

4. In order to distinguish City employees from vendors/contractors, all vendors/contractors who are provided a City email address will be assigned an email address with an -nc extension. For example, jsmith-nc@santa-clarita.com.

B. **No Right of Privacy**: The City respects the individual privacy of its employees. However, employee privacy does not extend to the employee's work-related conduct or to the use of City-provided equipment or supplies. Employees and any users should be aware that the terms of this Policy limit their privacy in the workplace.

The City's Electronic Communications Systems, Electronic Communications, and Electronic Storage are City property and are intended for City business. All Electronic Communications and Electronic Storage within these systems are the property of the City of Santa Clarita, regardless of the content, including any personal communications. The

City reserves the right to monitor the Electronic Communications Systems for any reason at any time without notice to the user(s), including the right to review, audit, and disclose all matters and content sent over and/or stored on Electronic Communications Systems.

As a result, employees and users should be aware that no Electronic Communications transmitted on the Electronic Communications Systems, or Electronic Storage contained within the systems, is private or confidential. Employees and users should have no expectation of privacy with respect to any use, including storage, business or personal, of the City's Electronic Communications Systems.

Employees and users should be aware that Electronic Communications and/or Electronic Storage can be copied, modified, and/or forwarded to others without the express permission of the original author. Therefore, employees and users must use caution in the storage, transmission, and dissemination of Electronic Communications outside of the City and must comply with all state and federal laws. Electronic Communications and/or Electronic Storage of the City may be recognized as official records in need of protection/retention in accordance with state and federal laws. All electronic communications are subject to the Personnel Rules and all state and federal laws, including but not limited to the California Public Records Act, open meeting laws, and the federal Electronic Communications Privacy Act.

C. Passwords: All passwords created by the user or issued to the user are for the purpose of communication and are not to be shared, given, or otherwise disclosed to any other person. Passwords must not be shared and will need to be changed on a regular basis when prompted by the Technology Services staff to ensure security. All security features contained within the City's Electronic Communications Systems such as passwords, codes, or delete functions will not prevent the City from accessing employees' business or personal Electronic Communications, stored or otherwise, on the City's Electronic Storage Systems.

D. Appropriate Use of Electronic Communications Systems: The City of Santa Clarita's Electronic Communications Systems are designed to facilitate City business and communication through the appropriate use of the Electronic Communications Systems and Electronic Storage thereon. The City values its Electronic Communications Systems and Electronic Storage, and takes security measures to safeguard them from corruption and illegal use, and to protect the City from any possible liability due to illegal use of the Electronic Communications Systems and Electronic Storage.

1. No user shall access the City's Electronic Communications Systems without reading and complying with the procedures set forth in this Policy.

2. No user shall attempt to install, delete, or modify any hardware or software nor access Electronic Communications Systems without having been granted proper authorization.

3. All users requesting authorization to access the City's Electronic Communications Systems, Electronic Communications, and/or Electronic Storage shall be given a copy of all related technology policies and shall sign an acknowledgement of the policies recognizing the parameters for compliance with those policies.

E. <u>Improper Use of Electronic Communications Systems</u>: It is the responsibility of each City employee (or user) to use the City's Electronic Communications Systems in a professional and courteous manner. The City forbids the use of its Electronic Communications Systems in a manner that violates any law, regulation, ordinance, or policy or procedure of the City. Electronic Communications Systems should not be used in any way that is offensive, harmful, or insulting to any person. Examples of prohibited uses include, but are not limited to:

1. Illegal or malicious activities;

2. Solicitation of funds;

3. Political messages or transmissions;

4. Messages or transmissions that violate the City's Policy Prohibiting Harassment, Discrimination, and Retaliation based on gender, genetic characteristics or information, race, color, national origin, ancestry, religion, creed, sex, physical or mental disability, medical condition, marital status, sexual orientation, gender, gender identity, gender expression, age over 40, pregnancy, childbirth, or related medical condition, family medical history, genetic information, military or veteran status or any other basis protected by applicable federal, state or local law;

5. Messages or transmissions that violate the City's personnel rules and/or another policy of the City, including, but not limited to, anti-discrimination policies and anti-harassment policies; drug-free workplace policies; or

6. Any other message or transmissions which are in any way inappropriate.

F. <u>Personal Use of Electronics Communications Systems</u>: The City's Electronic Communications Systems are primarily for the conduct of City business. Limited, occasional, or incidental use of the electronics communications systems for personal, non-business purposed is permitted only under the following circumstances:

1. Personal use may not interfere with the productivity of the employee or his/her co-workers;

2. Personal use may not involve any prohibited activity described in this Policy, or any other City Policy or Rule;

3. Personal use may not disrupt or delay the performance of City business;

4. Personal use may not consume City resources or otherwise deplete system resources available for City business purposes;

5. Personal use may not be used for personal employee gain or commercial ventures; and

6. Personal use may not support or advocate non-City-related business purposes.

If an employee's personal use of the City's Electronic Communications Systems results in a cost to the City, the cost must be reimbursed to the City by the employee.

G. Retention of Electronic Communication: No electronic communication shall be considered by the City to be retained in the ordinary course of business, with the exception of electronic communication containing content required to be retained by law.

It is the responsibility of the creator to determine if an electronic communication sent internally should be classified as a record that requires retention in accordance with the City Council approved Records Retention Schedule. It is the responsibility of the recipient of an electronic communication received from outside City sources to determine if an electronic communication should be classified as a record that requires retention in accordance with the City Council approved Records Retention Schedule. Once retention status is determined, transfer of the electronic communication to a printed hard copy is required prior to deletion or purge from the electronic communication system. Each user is provided a limited amount of storage for their email messages and a finite amount of network storage, which they must manage appropriately. Email messages are automatically deleted per the City's retention policy. There is no process in place to retrieve or recover messages once they have been deleted.

H. Access of Another Person's Electronic Communications: Employees may not intentionally intercept, eavesdrop on, record, read, alter, retrieve, receive, send, or use another person's Electronic Communications and/or Electronic Storage without proper authorization. Employees, including system administrators and Supervisors, may not, without authorization, peruse Electronic Communications and/or Electronic Storage of other employees.

I. Requests for Access to Employee's Data, Messages, and Phone Records: Requests for access into an employee's individual data, messages, and phone records will be made to the Human Resources Manager. The Human Resources Manager, if in concurrence with the Director or Personnel Officer, will forward the request to the Technology Services Manager for action.

J. City-Wide Web Site Guidelines: The external (or public) City of Santa Clarita site, and all domains owned and maintained by the City, represent a fundamental communication tool for providing critical City information. The goal of the collective web

sites is to encourage increased participation in City government and to help create a more vibrant community for residents and visitors alike. The internal intranet (or rNet) web site provides fundamental and critical information to all employees to assist in accomplishing the City's mission. Toward that end, the development and use of the City's sites are guided by these web site guidelines:

1. The City's Technology Services Division is responsible for advising City departments regarding the creation and implementation of their respective web sites, helping City departments to comply with the City's web guidelines, and maintaining and securing the City's web servers and web site. It is the responsibility of the Application Development team within Technology Services to ensure that department staff adheres to the web site guidelines.

2. To preserve the public nature of the City's web site and to avoid any perception that the City endorses or provides favorable treatment to any private person or business enterprise (hereinafter collectively referred to as "vendor"), no corporate or commercial logos or links to vendor sites will be allowed on the City's external web site, unless such link represents a mission critical partnership and is authorized by the City Manager. Exceptions may be made by Technology Services staff on a case-by-case basis.

3. Vendors contracted to create or maintain a web site for any City department shall be provided this policy and must follow all guidelines established for the City's web site.

4. The City's web site, and ancillary web sites, is for "official use" only. All information disseminated through the City's web sites must be related to the official duties and responsibilities of employees and City departments.

5. The Communications Division Manager must approve all ancillary web sites created for official use and the City employee responsible for the posted information.

6. The California Public Records Act applies to information processed, sent, and stored on the Internet. Confidential information should not be posted on the City's external web site.

No City employee or official may use any City web site for campaign-related purposes. Such campaign-related purposes include, but are not limited to, the following: statements in support or opposition to any candidate or ballot measure; requests for campaign funds or references to any solicitations of campaign funds; and references to the campaign schedule or activities of any candidate. No City official's web site may be linked to any private web site related to a candidate's campaign for elective office, but it may link directly to the home page of the Office of the City Clerk's election-related pages where general election and candidate

information can be found.

K. Internet Usage Policies: Authorization for Internet access is governed by Technology Services according to job classification and division. Any requests for additional Internet access, above and beyond what is customary for a job classification or division, must be requested through an employee's Supervisor. Authorization for Internet access for volunteers, vendors, contractors, and anyone else not in City employ must be approved by the Human Resources Manager. Once authorization is approved, the employee or user is responsible for the security of his/her account password and will be held responsible for all use or misuse of his/her account. Users must maintain secure passwords.

1. Appropriate Use of the Internet. Employees who are granted access to the Internet are expected to use this privilege in a professional and courteous manner. The prohibited uses of Electronic Communications Systems described in this Policy apply to the use of the Internet. All users should be aware that appropriate use of the Internet includes, but is not limited to, the following rules:

(a) Never use an account assigned to another user.

(b) Never make an unauthorized attempt to enter any computer.

(c) Never post, send, or provide access to any confidential City materials or information, unless authorized.

2. Improper Use of the Internet. Employees should be aware that the improper use of the Internet also includes, but is not limited to:

(a) Disclosing confidential information obtained in the course of employment;

(b) Accessing web sites or online content that may degrade, hamper, or impede on the performance and/or capacity of the City's Electronic Communication Systems;

(c) Accessing gross, indecent, obscene, harassing, pornographic, or sexually explicit materials;

(d) Accessing gambling sites;

(e) Accessing illegal drug-oriented sites; and

(f) The representation of yourself as someone else, real or fictional.

3. Social Networking Sites. The City reserves the right to limit access to certain sites deemed inappropriate. Should the need arise, users are obligated to cooperate with any investigation regarding the use of their computer equipment.

Questions regarding confidential or proprietary information should be directed to the Technology Services Manager. City management has the right to monitor and log all transactions in or out of the system. All security features contained within the City's Electronic Communication Systems such as passwords, codes, or delete functions will not prevent the City from accessing employees' Electronic Communications, stored or otherwise, on the systems.

L. Employee Terms of Use for City Mobile Devices: City-issued phones may be provided for the conduct of City business. All telephone equipment (land-line phones and cellular phones) shall be issued to personnel according to the needs defined in their job description.

Requests for City Issued Mobile Devices. Requests are to be made using the designated request form. Only department Directors may approve the issuance of a City mobile device for all regular and PTS staff. Only the City Manager or Assistant City Manager may approve the issuance of a City-issued mobile device to a non-employee.

Division Managers are responsible for reviewing and monitoring their staff's mobile device bills on a regular, usually monthly, basis. Division Managers are also responsible for documenting the issuance of a cell phone and its accessories, and ensuring that they are returned once the employee has exited the department.

The Directors may review which employees have cell phones and whether or not they still need them.

The following criteria should be considered in determining who needs a City-issued cell phone:

1. Business need for employee to use the device on a daily or regular basis;

2. The position requires the employee to respond to email while off-site;

3. The position requires the employee to respond to email after normal working hours;

4. The position works at, or is responsible for multiple facilities;

5. The position requires remote network monitoring responsibilities, such as Technology Services or Traffic staff; and

6. The position is a designated City Emergency First Responder

Permitted Uses:
The use of City cell phones by employees for making personal calls may be permitted, subject to the provisions of this Policy, if it does not interfere with the conduct of City business. The use of City's phones must be in accordance with the following procedures:

1. All calls should be limited to the shortest amount of time necessary to conduct City business.

2. All City employees must continuously strive to minimize costs.

3. Employees are not allowed to use City-issued phones in an illegal, illicit, or offensive manner.

4. Employees are not allowed to use City-issued phones to conduct personal for-profit business.

5. Safeguarding issued equipment is the responsibility of the individual employee. Misuse or abuse of equipment may be cause for disciplinary action and/or cost reimbursement.

6. Features on cellular phones such as directory assistance, busy signal confirmations, text messaging, and emergency interrupts should only be used for official City business and only when absolutely necessary. Misuse or negligent use of these features may be cause for disciplinary action and/or cost reimbursement.

Employees are not allowed to operate cellular telephones, laptop computers, navigational devices, or any other devices that may cause driver distraction when driving a City vehicle or when driving a private vehicle being used to conduct City business. Employees shall make every attempt to properly park their vehicle prior to using such devices. The only exception to this rule is if the employee uses a handsfree device.

If traveling internationally, the employee must receive Division Manager approval to add an international data/voice plan to their mobile device. If approved, the employee must reimburse the City for any additional costs incurred, unless access while abroad is necessary for City business. Technology Services must be notified prior to and upon return of any international travel to make any applicable international billing changes.

Any personal calls made from a City-issued phone will be the responsibility of the employee. Employees are responsible for identifying minutes of personal use and then reimbursing the City. The reimbursement amount should be a simple calculation of the per-minute rate charged for every minute of personal usage. This reimbursement should be made payable to the "City of Santa Clarita" and should be submitted as payment to the City cashier within ten (10) days of receiving the bill.

The City shall provide Management Analysts with a monthly cellular phone bill report for employees with City-issued devices within their department.

Employee must wipe the device and return with all passwords removed or provide all applicable passwords to Human Resources upon termination of employment.

M. Employee Use of Personal Cell Phone for City Business

1. Employees who elect to use a personally owned mobile device to conduct City business or access the City's email server for work related purposes must be aware that by doing so they are waiving certain privacy interests, and that City related emails, data, or other material located, stored, or transmitted on a personal mobile device are subject to all City Personnel Rules and Policies, all federal, state and local laws, including but not limited to the California Public Records Act and open meeting laws.

2. Non-exempt staff who conduct City business on personal time on a mobile device must obtain prior approval of their Supervisor, and must report said work on their timecard as time worked.

3. Employees who elect to use a personally owned mobile device for City business must retain all emails and data in accordance with the City's record retention schedule.

4. Employees who elect to use a personally owned device for City business should have no expectation of technical support from Technology Services beyond basic assistance connecting to the City's email server because they will not have the necessary access to troubleshoot service issues.

5. A stipend shall be available to eligible employees (see below). However, at the discretion of the City Manager, or designee, the stipend may be extended to other employees.

(a) City Manager, Assistant City Manager, and Department Heads

N. Telecommuting and Remote Access to City Electronic Systems:

1. Employees and users who access any of the City Electronic Systems remotely must comply with all City policies and procedures regarding the use of said systems regardless of whether the user is using a City-owned or personally-owned cell phone or computer.

2. Employees and users who are approved to use non-city equipment to access City Electronic Systems must ensure said devices have updated and working anti-virus software installed prior to attempting access.

3. Non-exempt employees must request approval from their Supervisor to access City Electronic Systems outside of their normal work schedule. Any such time, beyond de minimis use of less than 5 minutes, must be reported as time worked and be paid accordingly. De minimis use of less than 5 minutes need not be reported. This specifically includes but is not limited to checking, accessing, reviewing, composing, responding to, and forwarding any emails, Outlook items, or any other

City Electronic System for work-related purposes.

IV. VIOLATION OF POLICY

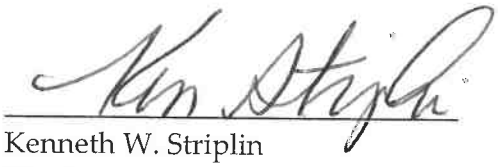
Violations of this Policy shall be reported to the Human Resources Manager, appropriate Director, and/or the Personnel Officer only. Any employee who accesses the City's Electronic Communications Systems without complying with the procedures set forth in this Policy or otherwise violated this Policy may be subject to disciplinary action, up to and including termination, as provided for in the City's Personnel Rules. In addition, misuse of the Electronic Communications Systems may, in appropriate cases, be referred for criminal prosecution.

V. EXCEPTIONS

There are no exceptions to this Policy without City Manager approval.

VI. AUTHORITY

By the authority of the City Manager.



Kenneth W. Striplin
City Manager