City of Palos Verdes Estates

Technology Utilization and Electronic Use Policy

Employee Acknowledgement: Name _____Date _____

Purpose

To establish policy and procedures for access to and use of the City's information technology and communications systems and equipment, as well as the retention and disposal of electronic communications. This policy covers Electronic Communications, Electronic Records, Voicemail, Internet, Intranet and Network Usage.

Application and Scope

This policy shall apply to all City elected and appointed officials, employees, volunteers, consultants, contractors and other individuals who are provided access to the City's information technology and communication systems, including, but not necessarily limited to, computers, peripherals, e-mail, telephones, and both hardware and software applications (collectively referred to hereinafter as "Users"). In compliance with federal and state law, this policy is not intended to and will not restrict employees from engaging in protected concerted activity, including discussing their wages, hours and working conditions with other employees. (Cal. Lab. Code §§ 232, 232.5)

Due to the sensitive and investigative nature of police operations and public safety records requirements, a distinct policy exists for such operations as part of the Police Department Policy Manual. To the extent that the terms of this policy included herein are in conflict with Police Department policy, Police Department Policy shall control for Police personnel.

Enforcement

The City Manager, his/her designee or, if necessary, the City Attorney shall be responsible for enforcing this policy.

Policy

The City's information technology and communication systems and equipment shall be used primarily for conducting City business, and are not intended for personal use. All electronic communications, including those communications placed on the City's Telephone, Internet, Intranet, Application Software and Network Systems, are the exclusive and official property of the City. The City reserves the right to retrieve, access, review, audit, copy and make proper and lawful use of any and all electronic communications transmitted through these systems or on any technology owned, issued or maintained by the City. For purposes of this policy, "electronic communications" shall include all messages, pictures, or attachments, and any and all activity and transactions transmitted over the City Internet as well as the City's calendaring, instant messaging, email telephone, voicemail, and other communication systems.

Users have no expectation of privacy in any electronic communication sent over, accessed or received on any City network information technology and communication system. Access to a database, service, voicemail or website requires a username or password shall not create an expectation of privacy if it is accessed through City owned computers, networks, telephones, software applications or equipment.

A. PROPER USE OF ELECTRONIC COMMUNICATIONS SYSTEMS, TELEPHONE, VOICEMAIL, INTERNET, INTRANET AND NETWORK RESOURCES

The City's information technology and communications systems and equipment may only be used for the following:

1. To transmit electronic communications which shall only be used for authorized City business activities. Such communications shall only contain information related to the accomplishment of City business or employee relations.

2. Job-related professional development, educational activities and information sharing with business, City partners, professional associations and professional colleagues that are incidental to User's duties are permissible.

3. Occasional non-business use of information and communication systems and equipment is permitted as a privilege provided by the City for the User's convenience, but shall not interfere with City operations, result in increased costs to the City or be conducted in a manner that violates this policy. Users shall have no expectation of privacy for this type of use of City information and communication systems and equipment.

4. Users should take reasonable care to prevent the introduction or spread of computer viruses into or through the City's communication and information technology systems and equipment. Users shall not without proper authorization attempt to disable or change any settings, preferences or configurations of anti-virus software that has been installed on City computers or equipment. Use of anti-virus software does not guarantee that a virus will not or cannot infiltrate the network. Viruses often enter as attachments to e-mails. Accordingly, Users are required to take extreme care not to open emails or attached files received from unfamiliar sources or with non-standard file extensions (exe," ".worm," ".dot," ".zip,").

5. To protect the security of the City network and systems, the City shall have the right to restrict program software downloads in the effort to maintain system standards and compatibilities.

6. The City shall have the right to establish a standard for and/or restrict the use computer peripherals (i.e.: flash drives, exterior storage devices, printers, monitors, keyboards, printer cards, video cards, local area network cards, modems, and enhancement or accelerator boards) to guard against errant computer viruses, malware and other invasions of the system. Peripherals brought into the environment and activated for purposes of police investigations and/or evidence, shall be secured and used in compliance Police Department policy for such purposes and identified/secured accordingly.

7. Each User is responsible for the management of his/her email mailbox and its associated folders, subject to the provisions of Section E of this policy.

B. PROHIBITED USES OF ELECTRONIC COMMUNICATION, TELEPHONE, VOICEMAIL, E-MAIL, INTERNET, INTRANET AND NETWORK RESOURCES

1. The following types of electronic communications are expressly prohibited. Any violation of this section may subject a User to disciplinary action or termination:

   a. Electronic communications that disrupt or threaten to disrupt the efficient operation of City business or administration. Such communications include, but are not limited to, those that publicize a personal dispute other than according to an approved grievance or complaint procedure, those that constitute insubordination, those that may harm working relationships, those that may take employees away from their assigned tasks, those that may undermine the City's ability to provide public services through its employees, those that harm the integrity of the system or network, those that could reasonably be expected, directly or indirectly, cause excessive strain on any of these resources or those that interfere with others' use of these resources.

   b. Electronic Communications that violate law, violate individual rights or that violate City policy or public policy of the State of California, are prohibited. Such communications include, but are not limited to:
      i. Those which are pornographic or obscene.
      ii. Those in conflict with the City's Sexual Harassment Policy or any other policy prohibiting discrimination, including harassment, on the basis of race, color, religion, sex, national origin, ancestry, age, physical disability, mental disability, medical condition, veteran status, marital status, sexual orientation or any other status protected by local, state or federal law.
      iii. Those that include the use of racial, religious or ethnic slurs.
      iv. Those intended to harass or annoy, or which are malicious, reckless or knowingly false.

   c. Threats to personal safety or which constitute a "credible threat of violence," as defined by California Code of Civil Procedure section 527.6(b) (2).

   d. Electronic communications that solicit or proselytize others for non-City or non-job related commercial ventures or products, religious or political causes, or that solicit funds or support for outside organizations or other non-job related solicitations.

   e. Electronic communications that result in any-one individual's private/personal enterprise gain or advantage for the User (such as an employee conducting business related to economic interests outside of City employment).

f. Electronic communications that disclose confidential, private or proprietary information, unless authorized to do so by the City Manager, his/her designee, or Police Department Policy.

2. The following activities are expressly prohibited. Any violation of this section may subject a User to disciplinary action or termination:

a. The use of a false identity (the name or electronic identification of another) unless such use is part of a Police Department investigation or is otherwise authorized by Police Department Policy.

b. The copying of City network security, operating system security and/or configuration files.

c. Any attempt to circumvent passwords, security, permissions, or rights on any internal or external system using the City's network, computers, or Internet access. If changes or additions to access are needed, contact should be made to the Finance Director, his/her designee or the City Manager.

d. The willful introduction of malicious code such as computer "viruses," "worms," "Trojan horses," "trap-door code," "denial-of-service attacks," or other disruptive and/or destructive programs into the City's computer systems or network.

e. Installing, duplicating or distributing copyrighted material using the City's network or computer systems without the appropriate licenses or permission from the copyright holder.

f. Deleting, examining, copying, or modifying files, e-mails and/or data belonging to, and existing within the private network dominion of, other Users without their expressed prior consent, except as noted in Section C.

g. Continuing a burdensome consumption of system resources, after receipt of a request to cease such activity.

h. Installing software or hardware on City information and communication systems, such as desktop or laptop computers, without authorization.

i. The physical movement and reassignment of desktops, laptops and printers, or other electronic equipment, without the written approval of the City Manager and/or his/her designee.

j. The physical removal of asset identification tags and/ or desktop/laptop

components including hard drives and processors.

C. PENALTIES FOR MISUSE OF ELECTRONIC COMMUNICATION SYSTEMS, TELEPHONE, VOICEMAIL, E-MAIL, INTERNET, INTRANET AND NETWORK RESOURCES

1. Failure on the part of any employee to comply with the provisions of this Policy may subject the employee to progressive disciplinary action in accordance with the City's personnel rules. Disciplinary action may include, but is not limited to, suspension or revocation of the privilege of using or accessing the system, if doing so would not otherwise materially impair the employee's ability to perform his or her job.

2. Failure on the part of any appointed official to comply with the provisions of this policy may constitute grounds for (a) the City Council to deny the official access to the system and/or (b) removal from that position.

3. Failure on the part of any non-employee, volunteer, contractor or consultant to comply with the provisions of this policy will constitute grounds for termination of their relationship with the City.

D. STATUS OF COMMUNICATIONS

1. Electronic communications in general are not confidential and are subject to review by City management as set forth in this Policy.

2. Electronic communications including emails, text messages, and records of cellular and telephone calls are subject to disclosure by the City to persons/entities outside of the City pursuant to court or administrative order, subpoena, Public Records Act request, and/or may be used as evidence in court or as part of an internal or external investigation. The City, in the sole discretion of the City Manager and/or the City Attorney, may raise objections to the disclosure of electronic communications. When the City is obligated, directed or chooses to disclose electronic communications, the content of electronic communications and/or documents may be disclosed within or outside of the City without employee permission or knowledge, although the City may, but is not obligated to, provide notice to the employee. Users are advised that any use of the City's electronic communication systems for non-City purposes, outside of the conditions of this policy, is at their own risk and always subject to disclosure.

3. The City Manager or his/her designee has the authority to access communications in the system at any time for any lawful City business-related reason, except as otherwise provided for in this Policy.

4. The City Manager or his/her designee has unlimited access to protect system security or the City's property rights.

E. E-MAIL MESSAGE SIGNATURE BLOCK AND DISCLAIMER

1. All e-mails generated by non-safety employees utilizing City equipment, systems and/or resources must contain the author's signature block in a form substantially comparable to the following:

Name
Position/Title
City of Palos Verdes Estates
340 Palos Verdes Drive West
Palos Verdes Estates, CA 90274
310. Phone number/Extension Fax: 310.fax number

www.pvestates.org

2. All e-mail generated by non-safety Users utilizing City equipment, systems and/or resources must contain the following disclaimers following the author's closing/signature:

This is a transmission from the City of Palos Verdes Estates. The information contained in this e-mail pertains to City business and is intended solely for the use of the individual or entity to whom it is addressed. If the reader of this message is not an intended recipient or the employee or agent responsible for delivering the message to the intended recipient, and you have received this message in error, please advise the sender by reply e-mail and delete the message.

WARNING: Computer viruses can be transmitted by e-mail. The recipient should check this e-mail and any attachments for the presence of viruses. The CITY OF PALOS VERDES ESTATES accepts no liability for any damage caused by any virus transmitted by this e-mail.

3. The disclaimers must be in a clearly legible font (e.g., Veranda, Times New Roman, Arial, etc.) no smaller than the font size of 7.5.

F. CITY COUNCIL E-MAIL CORRESPONDENCE

This Section is intended to describe guidelines and practices for City Council e-mails and e-mail correspondence.

1. The City will provide an individual e-mail address for each member of the City Council at *name@pvestates.org*. All e-mails sent and received from this address, along with all other electronic communications, are subject to this policy as well as records retention, the Public Records Act, the Ralph M. Brown Act and other State and Local requirements.

2. Upon the provision of City Council e-mail address, the use of generic personal e-mail address (e.g., aol.com, gmail.com, yahoo.com) by Councilmembers is discouraged in recognition of Public Records Act request impacts, back-up archiving, and processes.

3. Individual City-provided Council e-mail addresses are for City-related correspondence, to and from a members of the City Council. Each member of the City Council will have personal access to the e-mails by establishing his/her personal password access; City staff (including the City Manager) will not access the e-mails, unless directed by the City Council, the individual City Councilmember, or otherwise required by law, such as a subpoena or Public Records Act request.

4. Technical Information Technology support will be made available by the City to each member of the City Council for matters that relate to managing the City e-mail addresses.

5. Because City staff will not generally have access to City Councilmember e-mails, City staff members shall not be able to provide a City response to inquiries sent only to the City Council members. As such, City Council members should forward e-mails to the City Manager (or designees) if a City response is desired.

    i. The City Council Guidelines, policies, and specifically, the roles and responsibilities of the City Council, City Manager and City staff in relation to City business pertain when members of the City Council respond to e-mails.

    ii. If a City staff member is requested to respond to an individual e-mail, the City staff member in question may be unaware whether the same or a similar e-mail was sent individually to each member of the City Council. Therefore, City staff members will use their best judgment to determine if the e-mail was sent to other members of the City Council in determining if it is necessary to forward the response to each City Council member.

6. The City will also maintain a group e-mail address *CityCouncil@pvestates.org*. E-mails received at this address are received by the City Manager's Office. They will be reviewed by City staff, and circulated to members of the City Council as addressed. As appropriate to the e-mail, City staff will respond to e-mails with a City response from an individual e-mail address; accordingly, the response will be forwarded to City Council members.

G. E-MAIL ETIQUETTE

This Section is intended to set forth guidelines for e-mail etiquette. Repeated failures to adhere to the below guidelines may subject the employee to disciplinary action.

1. Communications both internally and externally should maintain a professional image for the author and the City.

2. Messages should be addressed to the proper person. Confirm the list of persons being e-mailed before responding "REPLY ALL." E-mail should not be used for broadcast purposes unless the message is of interest to all or most of the users.

3. Capitalize words only to emphasize an important point or to distinguish a title or heading. Capitalizing whole sentences or paragraphs is generally interpreted as shouting.

4. Remain cautious to avoid using sarcasm, humor or slang. Without face-to-face communication, humor may be misinterpreted as criticism or harassment. Also carefully read what others write. The perceived tone may easily be misinterpreted.

5. Some messages, especially those written in "the heat of the moment," are best unsent. Avoid sending angry or sarcastic messages or using e-mail to let off steam.

6. Employees play a vital role in protecting the City's network from computer viruses and other security threats. Please make every effort to exercise safe computing use practices. Ask for assistance whenever a problem is suspected.

7. If an employee anticipates a scheduled absence, an "Out of Office" auto-response message shall be prepared. The length of the absence, anticipated return to the office, as well as contact information for an individual covering in the employee's absence should be included in the auto-response. This is optional for police personnel in deference to police operations confidentiality needs.

H. TELEPHONE AND VOICEMAIL ETIQUETTE

This Section is intended to set forth guidelines for telephone and voicemail etiquette only.

Repeated failure to adhere to the below guidelines may subject the employee to disciplinary action.

1. Employees are to be courteous, respectful and attentive while on the telephone.

2. Voicemail is not to be used as a substitute to answering a City telephone during regular business hours.

3. Absent unusual circumstances, voicemail messages should be returned by the end of the business day of receipt but in no event later than the staff person's next working day.

4. Irate callers shall be treated with special care. Employees should attempt to identify their primary complaint quickly and exercise patience/restraint in crafting a response.

5. Callers may be disconnected if the caller refuses an employee's request to refrain from using abusive or profane language, unreasonably refuses to conclude the conversation, is unreasonably repetitive, or otherwise is not communicating in a manner that is capable of being understood.

6. Voicemail greetings shall contain the staff member's name, title and "City of Palos Verdes Estates." This is optional for police employees in deference to police confidentiality needs.

7. If an extended absence is expected, an alternate secondary message shall be prepared. The alternate message shall specify the length of the absence and the employee's anticipated date of return to the office, as well as the information included in the standard primary greeting. This is optional for police employees in deference to police confidentiality needs.

I. ELECTRONIC RECORDS MANAGEMENT AND RETENTION

1. Information technology and communication systems and equipment are media for transmission of communication and are methods to send, receive, or temporarily store correspondences. E-mail is a business tool that provides an efficient and effective means of intra-agency and inter-agency communications. Communications generated through these systems are not City records retained in the ordinary course of business until the communication has been printed and retained or downloaded into a local network file folder and specifically recognized as a City record subject to retention. The retention of communications generated through these systems is expressively governed by this Policy. Users are responsible for consulting the Records Retention Schedule to determine if a specific e-mail and its content needs to be retained.

2. All emails will be deleted/purged from the City's e-mail server, beginning at a retention term of ninety (90) days and progressing to thirty (30) days, after a phase-in period defined below. This shall apply universally unless a particular e-mail is required to be kept for a longer period pursuant to the Records Retention Schedule or applicable law. 90 days after this policy adoption by City Council, a 90 day e-mail retention will be in effect, 60 days later a 60 day e-mail retention will be in effect. 30 days later, emails over 30 days old will be deleted off the server. As such, well within a year after adoption, the City will have in effect a 30-day retention/purge schedule in place. However, the City Manager and/or the City Attorney retain the discretion to temporarily modify or suspend this retention/purge as necessary to preserve electronic communications pursuant to federal and state law regarding the preservation of evidence.

3. Each User is solely responsible for the management of his/her mailboxes, just as they are responsible for sorting through paper mail in their in-boxes from the US Post Office or inter-office memoranda. E-mail is not a permanent storage medium and staff members are expressly forbidden to use it as such. E-mail system in/out-boxes shall be emptied on a regular basis, after records have been appropriately saved, as outlined below. The City technology division will provide non-email server archival capabilities within the network to allow for the paperless storage of files subject to retention. ***E-mail archival and maintenance, as outlined below, is the primary responsibility of the direct e-mail recipients (those addressed on the "to" line of the e-mail) and not that of those cc'd in the transmission.***

a. E-mail messages which relate to the conduct of the public's business and which are intended to be retained in the ordinary course of the City's business are recognized as official records in accordance with the California Public Records Act. The City's e-mail system was neither designed for, nor is it cost effective to, maintain long term storage, or e-mail communications. The City will maintain all e-mail messages determined by staff to be official records (those that have a material impact on the conduct of the City's business or that are otherwise required to be retained by law) as designated in the Records Retention Schedule by printing and ***saving them in a paper file, or by archiving them electronically in network based archive drives to be provided by the City's technology division***. These records shall be managed in accordance with applicable law and City policies (i.e. separate and protect confidential attorney/client privileged communications, etc.). E-mails should only be sent or forwarded to appropriate persons with a need to know the information in order to conduct City business.

b. E-mail communications that are left within the e-mail system will be automatically deleted after a period of 90 days, in the initial implementation phase, and 30 days when the policy has completed the phase in cycle noted above. Under the California Public Records Act, the City owes a duty to disclose "public records" to members of the public, upon request (Cal. Gov't Code §§ 6250 *et seq.*). The Act defines "public records" as "any writing containing information relating to the conduct of

the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." (Gov't Code § 6252(e).) Accordingly, text messages and e-mails regarding City business that may constitute a public record shall not be sent on personal cell phones, smart phones, personal digital assistants (PDAs), or personal e-mail accounts as they cannot be properly managed and retained by the City. However, the use of personal devices to send and receive electronic messages, including e-mails, regarding the conduct of City business may subject such communications to disclosure under the Public Records Act.

c. Employees shall not commingle e-mail or other privileged correspondence or memoranda from the City Attorney's office with public documents (documents that are accessible to the public). These e-mails are subject to the attorney-client privilege and/or the attorney work product doctrine. Employees shall not forward e-mails and/or attachments thereto from the City Attorney's office without prior approval from the City Attorney, unless the e-mail itself expressly states that it is to be forwarded or shared.

d. If an employee separates from City employment, or transfers to another department, the records stored in the e-mail account of that employee shall be accessible to and the responsibility of that employee's final supervisor. The supervisor may review the e-mails of the former employee, ensure that the contents of the employee's e-mail account are preliminary drafts not retained in the ordinary course of business, and then authorize the deletion of the e-mails (after appropriate records are retained for their retention period, if appropriate.). Upon receipt of notification from the Human Resources Department that an employee has separated from the City, the Information Technology Department shall immediately ensure that the former employee does not have access to City e-mail and that the supervisor has access to the former employee's email address. Should a departing employee's desktop and/or laptop be subject to reassignment to another employee, the official cleansing of resident component hard drives and data files will be coordinated exclusively with the City's information technology division.

J. RESPONSIBILITIES

1. The City expects all Users to be responsible for adhering to this policy. All Users will be provided a copy of this policy, upon receipt of access to the computer network.

2. It is the responsibility of the City Manager and any other supervisory employees to use their best efforts to take the necessary and proper steps, including disciplinary action, to maintain a positive and effective working environment for all City employees in accordance with this policy.

3. Any supervisory staff member who observes or receives a complaint of electronic communication, E-mail, Internet, or network misuse, as specified in this policy, whether formal or informal, oral or written, shall endeavor to resolve the problem, and then report the matter to the City Manager, Human Resources Department or, if necessary, the City Attorney. Supervisory staff shall not independently review or investigate an employee's electronic communications, but instead, shall coordinate any such review with the City Manager, Human Resources Department or, if necessary, the City Attorney.

4. The City Manager or designee is responsible for promptly initiating an investigation after receiving a report of an unresolved complaint or incident of any misuse as delineated in this policy.

5. Non-safety users who inadvertently receive unwelcome offensive, inappropriate material or materials that violate policy should report the receipt and content of the communication to the City Manager, Police Chief, Human Resources Department or, if necessary, the City Attorney. Safety users should report such items in line with the existing chain-of-command protocol for ultimate reporting to the Police Chief as necessary. The User should preserve the offensive or inappropriate communication for investigative purposes, but should not forward it to individuals not involved in a City-initiated investigation.