



ADMINISTRATIVE REGULATION

Office of the City Administrator

Number	605
Sections	108
Effective Date	8/1/07
Responsible Department	Information Systems
Review Date	8/1/12

SUBJECT: Computer System, E-Mail, and Internet Network Use

1. **Purpose:** This policy governs the operation and/or use of the City of Huntington Beach's information technology including, but not limited to, computers and computing systems, networks, software, internal and external e-mail, the Internet and intranet, as well as communications-related tools and other electronic media such as Personal Digital Assistants (PDAs), phones, cell phones, pagers, fax, copiers, and voice mail collectively referred to as information technology systems.
2. **Authority:** Section 401 of the Huntington Beach City Charter.
3. **Application:** This policy applies to all elected and appointed officials; employees (regular, extra-help, and temporary); contractors; volunteers; and other individuals who are provided access to the city's information technology, collectively "users." Third parties should only be provided access to the city's information technology as necessary for their business purposes with the city and only if they agree to abide by all applicable rules.
4. **Definitions:** For the purposes of this policy, the following definitions shall apply:
 - 4.1. **Authorized User** - A city employee, or any person who has signed the User Authorization and is approved to utilize the specific system as part of their assigned official duties including, but not limited, to full or part-time employees, elected and appointed officials, volunteers, contract support personnel, and consultants.
 - 4.2. **Authorized City Representative** - Means each user's respective department head or the Information Services Director as appropriate.
 - 4.3. **E-Mail** - Shall mean any computerized system or software designated for the transmittal of written messages. Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of communication across computer network systems between or among individuals or groups. Also included are services such as list servers, electronic bulletin boards, and news groups.
5. **Policy** - It shall be the policy of the City of Huntington Beach that the use of all electronic media including city computers and PDAs, internal and/or external e-mail, and/or access to the Internet or intranet, shall be for job-related purposes.
 - 5.1. Information technology systems are the sole property of the city. The city reserves all rights, including termination of service without notice, on all systems that it owns and operates. The city may restrict access to its systems without prior notice and without consent of the user.

This policy shall not be construed as a waiver of any rights of the city, nor shall it conflict with applicable law.

- 5.2. The city, as provider of information technology systems, reserves the right to specify how the city's network resources will be used and administered to comply with this policy and other city rules, policies, resolutions, and ordinances.
- 5.3. The city may conduct reviews of the content of messages and files stored on network drives and web sites visited on the Internet, including random reviews, when in the exercise of its business judgment the city determines that it would be prudent to do so. The city further reserves the right to inspect, repair, service, and remove non-city business files from all servers and workplace computers. The city reserves the right to review and disclose all information transmitted through these systems. The city may control access to its systems in accordance with the laws of California and the United States and the policies of the city. The city reserves the right to access all information stored on all city systems for any reason.
- 5.4. The information sources accessible via the Internet are worldwide and constantly growing in kind and number. The city reserves the right to restrict access to any of these sources if/when, in its sole discretion, the city determines a source is not necessary to facilitate city business. Restriction of a specified source does not imply approval of other non-restricted sources. Employees are prohibited from intentionally accessing any Internet sites that are discriminatory or offensive in nature or promote or advocate any form or type of discrimination. Employees are prohibited from posting personal opinions on the Internet using the city computer system's access without the City Administrator or his/her designee's approval. Any attempt to access a website that has been filtered by the network website filtering software, or any attempt to bypass the city network filtering measures by the use of software or hardware designed for the purpose of bypassing city filtering measures, is prohibited. Should the need arise to access a filtered/prohibited website, the employee should contact his/her supervisor and gain official authorization to have the Director of Information Services allow the necessary access for the prescribed period of time.
- 5.5. **Suspension of Privileges** - The city may suspend without notice information technology system privileges of a user for reasons relating to suspected violation of city policies; contractual agreements; or local, state, or federal laws. This includes, but is not necessarily limited to, instances of employee termination, investigations of information technology systems usage misconduct, or when the user is deemed to represent a threat to any component of the systems. Access will be restored when deemed appropriate by the city considering the circumstances surrounding the suspension.

6. **PROCEDURE:**

- 6.1. City computers or information technology systems shall only be used for purposes relating to achieving the city's mission and shall not be used for personal business except as provided herein. Computer and communication systems are business tools to be used in accordance with generally accepted business practices; current laws including, but not limited to, the California Public Records Act; and consistent with the city's other policies including, but not limited to, the city's Document Retention Policy.
- 6.2. Information received or transmitted by any computer or communication system, whether deleted or not, may be logged, recorded, or otherwise monitored and is subject to disclosure based on the provisions of the Public Records Act and/or approval of the City Attorney.
- 6.3. Electronic mail shall not be used as a permanent storage medium. Electronic mail and calendar items are purged on a regular basis. Automatic and manual archiving of e-mail will not be permitted. Network and local drive storage of e-mail files, other than outlined in section 6.5, will be disabled.

- 6.4. E-mail record items will not be maintained on the city's e-mail server equipment or back-up media longer than 90 days. Calendar items will be maintained for a maximum of 365 days. Individual employees are responsible for printing, or electronically filing and retaining, e-mails that may be classified as official city business records. E-mails regarding policies, decision making, and contracts, or anything that in the employee's judgment could qualify as official city business, should be retained.
- 6.5. E-mail messages that are required or intended to be retained for long-term storage should be placed in the appropriate subject file, either electronically or in hard copy. Such e-mail messages will be subject to the city's Record Retention Schedule and may become public records unless exempt from disclosure under other applicable provisions of the Public Records Act, e.g., personnel files, attorney-client communications, deliberative process, etc.
- 6.6. To protect against security threats and legal liability, e-mail communication must be handled in the same manner as a letter, fax, memo, or other city communications. All e-mail messages distributed through the city's e-mail system are considered city property. E-mail messages may not contain content that may be considered offensive or disruptive unless work related. This includes, but is not limited to, obscene or harassing language or images; racial, ethnic, political, sexual, or gender-specific comments or images that one may find offensive. Some city department employees may be able to send and receive such messages due to the nature of their work – for example, Police Department or City Attorney staff.
- 6.7. E-mail, either internal or external, shall only be used for purposes related to achieving the city's mission and shall not be used for personal messages or personal business. The exception for those authorized to send and receive outside e-mail would be short and infrequent messages; for example, to arrange or confirm appointments, correspondence with other governmental agencies, inform family of work hours or overtime assignments, etc., as long as it does not interfere with city business or job performance. Use of e-mail must be in accordance with all other information technology systems policy and procedures.
 - 6.7.1. Examples of acceptable, incidental personal use of city information technology include:
 - E-mail to notify family of a schedule change when an employee traveling on city business is delayed due to official business or a transportation delay.
 - An employee is required to work overtime without advance notice and e-mails to advise his/her family of the change in schedule or to make alternative transportation or child care arrangements.
 - An employee exchanges e-mail with family members (or those responsible for them, i.e., a school or day care center) to make certain of their well being and/or safety.
 - The employee e-mails businesses that can be reached only during normal working hours, such as a local government agency or a physician.
 - An employee e-mails businesses in the area to arrange for emergency repairs to his or her residence or automobile.
 - 6.7.2. Employees should check with their supervisor if in doubt about the appropriateness of a personal e-mail or other use of information technology systems.
 - 6.7.3. Allowed personal use does not include:
 - Usage for private gain, or in connection with compensated outside work, game playing, stock trading, or chat rooms. Personal use of the city's information technology systems is at the users' own risk and may be accessed, reviewed, copied, deleted, or disclosed by the city. The city does not permit use of city information technology systems for political or religious activities; sending messages or information that is in conflict with local, state, or federal law; applicable regulations of the network being used; city policies, rules, or procedures; unauthorized attempts to access data or break into any city or non-city system, and theft or unauthorized copying of electronic files or data. Harmful activities such as, but not limited to the following, are prohibited:

creating or propagating viruses; disrupting services; damaging files; and intentionally destroying or damaging equipment, software, or data belonging to the city.

- 6.8. All messages from city information technology systems must appropriately identify the sender. Information technology systems may not be used to intentionally misrepresent one's identity. E-mail shall not be sent under another user's name without authorization. Another user's e-mail shall not be read unless there is a city purpose for doing so and is authorized by a supervisor. No previously sent e-mail message shall be changed without authorization from the original author.
- 6.9. Computer software protected by copyright is not to be copied from, into, or by using city-computing facilities, except as permitted by law or by the contract with the owner of the copyright. No software may be installed, copied, or used on city resources except as permitted by the owner of the software and the express permission of the Information Services staff. No information technology systems equipment or software is to be purchased without the review and approval of the Information Services Department.
- 6.10. Access to city information technology systems equipment and resources by recognized employee organizations is allowed consistent with this policy's references to non-work uses and any provisions in an applicable M.O.U. Access shall be authorized only to the extent that union business is limited to those lawful activities that pertain directly to the employer-employee relationship and not such internal organization business such as soliciting membership; campaigning for office and elections; and shall not interfere with the efficiency, safety, and security of city operations. Employee organizations, and those representing them, shall have no greater access to use of computer resources than employees of the city. Use of city information technology systems to communicate between union representatives and city representatives is considered city business and shall be allowed during regular duty hours. Union use of the city's information technology systems is at the user's own risk and may be accessed, reviewed, copied, deleted, or disclosed by the city.
- 6.11. Users will ensure that all information technology systems assets: computer, monitors, laptop computers, PDAs, printers, and other devices that are assigned to or regularly used by them, are maintained and used in a manner consistent with their function and such that the possibility of damage and/or loss is minimized. Whenever possible, all portable computing equipment: laptop computers, PDAs, or other handheld computers, will be maintained under the direct supervision of the user that they are issued to. The equipment must never be left unattended in locations such as airports and hotel lobbies. When equipment must be left unsupervised, it must be made as inconspicuous as possible. Whenever practical, the computer shall be secured with the supplied security device(s).
- 6.12. Users are expected to report unauthorized access, including unauthorized access attempts or other improper usage of city computers, networks, or other information processing equipment. If a user observes or receives a report of a security or abuse problem with any city computer or network facilities, including violations of this policy, the user must take immediate steps as necessary to ensure the safety and security of information resources by contacting your immediate supervisor and/or the Director of Information Services.
- 6.13. Instant Messaging (IM) services including, but not limited to, MSN Messenger, AOL Instant Messenger, and ICQ, for example, may not be used on city computers. IM poses virus and security risks.
- 6.14. Whenever an official or employee possesses confidential information, the official or employee has an obligation to take all reasonable and necessary steps to protect the confidentiality of the information and minimize the likelihood of inadvertent transmission of the confidential information to unintended recipients. If an official or employee has any question regarding the implementation of this section, contact the City Attorney's office. Employees must exercise caution when creating or transmitting city business information electronically. Business information may not be transmitted to employees or other individuals who are not authorized

to receive such information. Electronic mail which contains confidential attorney-client information may not be disclosed to non-city personnel except the City Attorney's office, unless so authorized by the City Administrator or his/her designee, or as required under law. If an employee is unsure as to whether a communication is authorized, it is the employee's responsibility to inquire with their supervisor or the City Attorney as appropriate.

6.14.1. Brown Act

The Brown Act requires all meetings of the legislative body of a local agency to be open and public, and all persons must be permitted to attend such meetings with only a limited number of explicit exceptions. E-mail is a form of communication that may create a meeting subject to the provisions of the Brown Act. The following procedures are to be followed:

Council members and commissioners may use city e-mail systems and other services to distribute information, schedule meetings, and communicate on an individual basis with city staff provided that positions are not polled and decisions that require public deliberation by the full Council or commission are not made.

A maximum of less than a quorum of the Council or commission may communicate regarding any public business outside of a legally posted open public meeting; however, great care should be used to avoid the communication by a quorum of members on any such topic.

City Council members and/or commissioners may not make a collective decision, develop a collective concurrence on a matter, or take an actual vote via city e-mail systems or services.

A quorum of City Council members and/or commissioners may not make any series of communications regarding a decision, collective concurrence on a matter, consensus, or vote via city e-mail systems or services. Such activities constitute a serial meeting in violation of the Brown Act.

- 6.15. Employees may request permission to have remote access to the city's information network. Permission will be granted on a case-by-case basis by their department head. Employees with permission will work with the information systems staff for training on using their access. Any remote access to the city's network is strictly for business-related purposes and is not to be shared with any individuals who are not employed by the city.
- 6.16. Computers should be locked via the operating system, either manually each time users leave their desks for any period of time, or automatically using a password-protected screen saver. Computers should be left on at the end of each workday, but monitors should be turned off. This protects employees and the security of the system from someone else accessing the system using a valid username and password. Information Services staff may ask users to remove their screen saver passwords in order to perform installations, diagnostics, repairs, replacements, upgrades, or maintenance. Once completed, the user is to immediately change it back to a unique and secure password.
- 6.17. When a permanent or temporary employee or contractor is added to the electronic mail system and network, the department in which the employee resides completes the *Network User/Security Account form* on the Surfnet Forms & Templates section and sends it to Information Services Administration.
- 6.18. When an employee is separated from service, the following steps are taken:
If the department head has not already requested and received the employee's password, he or she will obtain the employee's password.
The department head or his/her designee will make a timely inspection of the employee's files and copy any files from e-mail and network drives which the department wishes to retain. Information Services staff will delete the employee's electronic mail and files contained in the city network unless requested to do otherwise by the department head. Back-up storage of these files will be retained offline.

7. Procurement:

- 7.1. Procurement of computer equipment, software, or telecommunication products, including phones and cellular phones, shall be procured through an e-mail request to the Information Services Helpdesk. Such requests will go through the standard technology purchasing process as posted on Surfnet. With the exception of Information Services staff, city procurement cards, credit cards, or petty cash shall not be used to purchase these items.
- 7.2. Information technology consumable items: toner cartridges, including diskettes, zip disks, CDs, DVDs, tape cartridges, and paper, do not require Information Services Department review and approval.

8. VIOLATIONS:

- 8.1. Violation of any provision in this policy will be reviewed on a case-by-case basis and may result in revocation of privileges, suspension, termination, and/or criminal prosecution. Failure on the part of any contractor, consultant, or non-employee to comply with the provisions of this policy will constitute grounds for revocation of privileges, termination of their contract, and/or criminal prosecution.

As a condition of using the city's computer system, the e-mail system, and the Internet network, all users must sign the respective Use Policy form attached.

(Original Signed) 
 Penny Culbreth-Graft, DPA City Administrator

Action Being Requested: [Click Here To Elect Action Being Requested](#)

Today's Date	Requested Date of Completion
24 September 2007	
User's Name	User's Title
Requestor's Name (if different from above)	User's Department

Option 1 – Model the New User After the Following Existing User (Provide the name of current employee)	
Option 2 – Custom User Configuration or Re-Configuration (Limit or grant access rights to the appropriate network resources as indicated below)	For One World, JDEdwards: (Please specify "Group" or call extension 5356.)