ADMINISTRATIVE REGULATION
Office of the City Manager

Number	**AR 605**
Responsible Department	**Information Services**
Effective Date	**July 9, 2019**
Latest Revision Date	**November 31, 2023**
Next Review & Reauthorization Date	**November 31, 2025**

SUBJECT: Email & Computing Resource Use

1. **Purpose:** This policy governs the operation and/or use of the City of Huntington Beach's information technology resources, including, but not limited to, computers and computing systems, networks, software applications, internal and external e-mail, the Internet, and Intranet. This also encompasses communications-related tools and other electronic devices/media such as tablets, smartphones, desk phones, cell phones, pagers, fax machines, copiers, printers, and voice mail, collectively called information technology (IT) systems.

2. **Authority:** Section 401 of the Huntington Beach City Charter.

3. **Applicability:** This policy applies to all elected and appointed officials; City personnel; and other individuals provided access to the City's information technology, collectively known as "Authorized 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** - All elected and appointed officials and City personnel, or any person who has signed the *Policy Agreement Declaration* ***(Attachment 1)*** and is approved to utilize the specific system as part of their assigned official duties.
   - **4.2. Authorized City Representative** - Each user's respective Department Head or the Chief Information Officer (CIO) or designee, as appropriate.
   - **4.3. Cloud** - Any service/resource accessed from the Internet that provides data storage, computing services, servers, and other technology infrastructure.
   - **4.4. Confidential Information** – Information of a sensitive nature intended for recipients with a business need-to-know that may include, but is not limited to, personal content such as medical, recruitment, disciplinary, and performance information; attorney-client privileged communications; and other protected information. Unless exempted by law, some types of confidential information may be subject to legal inspection and/or disclosure requirements.
   - **4.6. IT Devices** - This term encompasses a broad range of electronic devices used for various purposes in computing, communication, and information processing including but not limited to smartphones, tablets, PCs, desk phones, and printers.

5. **Policy:** It shall be the policy of the City of Huntington Beach that the use of all IT devices and e-mail, and/or access to the Internet or Intranet, shall be for job-related purposes.

5.1. IT 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 the 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 a provider of IT systems, reserves the right to specify how the City's computing resources will be used and administered to comply with this policy and other City rules, policies, resolutions, and ordinances. This includes cloud as well as on-premise systems.

5.3. The City provides a free Wi-Fi Internet access to the public at the Civic Center and other City facilities, which is managed by the Information Services (IS) Department. Public users at the City Libraries must agree to the City's Internet use guideline/disclaimer before their access and use of the public Wi-Fi.

5.4. The City may conduct reviews of the content of messages and files stored on network drives and websites visited on the Internet, including random reviews. 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 C City policies. The City reserves the right to access all information stored on all City systems for any reason.

5.5. The City reserves the right to restrict access to any Internet information sources if/when, at its sole discretion, the City determines that a source is not necessary to facilitate City business. Restriction of some sources does not imply approval of other non-restricted sources.

5.5.1. Employees are prohibited from intentionally accessing any Internet sites that are discriminatory or offensive or promote or advocate any form or type of discrimination.

5.5.2. Employees are prohibited from posting personal opinions on the Internet using the City computer system's access without the City Manager or designee's approval.

5.5.3. Any attempt to access a website that has been filtered by the network website filtering software, or any attempt to bypass the City's network filtering measures by using software or hardware designed for the purpose of bypassing such 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 CIO or designee allow the necessary access for the prescribed period of time only.

5.6. Authorized Users are forbidden from disabling or circumventing any computer-related security measure unless authorized by the Information Services (IS) Department.

5.7. The City may suspend without notice IT system privileges of an authorized 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 a threat to any component of the systems. Access will be restored when deemed appropriate by the city, considering the circumstances surrounding the suspension.

5.8. The City's network security devices decrypt network traffic to prevent security threats. This includes but is not limited to: personal email and banking information accessed through devices provided by the City. Decrypting network traffic allows for effective scanning for potential threats and protects the network from malicious activities. This process is carried out solely for security purposes, and all data handling will be conducted in accordance with relevant privacy laws and the City 's data protection policies.

6. Procedure:

6.1. As a condition of using any the city's computing resources, all authorized users must fill out and sign the *AR 605 Policy Agreement Declaration* (**Attachment 1**), which is part of the City's onboarding process where acknowledgement of receipt can be done electronically.

6.2. City computers or IT 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 (CPRA) and consistent with the City policies including, but not limited to the City's Records Retention Policy/Schedule.

6.3. 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 CPRA and/or approval of the City Attorney.

6.3.1. If Authorized Users believe information transmiteed via email or any other communication system is confidential or privileaged, they shall indicate prominently on the top of such communication in capital letters such as CONFIDENTIAL or PRIVILEAGED. This assists the City Attorney's Office to sort through information; however, it does not guarantee the exemption of the CPRA or the City's review.

6.4. Policies and Procedures related to E-mail

6.4.1. Emails should not be saved/archived outside of Outlook, including on departmental shared drives, personal drives, or desktops, to ensure they are included in public record request searches.

a. Email and calendar items older than one year will be automatically purged from employee mailboxes by default.
b. Every email preserved must have a clear and specific reason for its retention. Archiving emails in bulk is prohibited unless each individual email within that bulk meets a specified retention criterion.
c. Detailed procedures for archiving emails can be found on the Email Policy Information page:https://huntingtonbeachca.sharepoint.com/:u:/r/sites/HelpDesk/SitePages/Email-Policy-Information.aspx.

6.4.2. Unless exempt from disclosure under applicable provisions of the CPRA, (personnel files, attorney-client communications, deliberative process, etc.), the user is responsible for ensuring that e-mail with content that is subject to the City's Record Retention Schedule be placed in the appropriate subject folder, either electronically or in hard copy, for retention as per the schedule.

6.4.3. 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 communication. All e-mail messages distributed through the city's e-mail system are considered City property. Offensive or disruptive emails should not be sent. 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 (Please refer to the City's related policies - *Administrative Regulations 922 Anti-Harassment, Discrimination and Retaliation Policy and 924 A Respectful Workplace Policy*).

Exceptions may be made due to the nature of their work, for example, Police Department or City Attorney's Office.

6.4.4. The City's email system shall only be used for purposes related to achieving the City's mission and shall not be used for personal messages or personal business. Use of e-mail must be in accordance with all other IT systems policies and procedures.

6.4.5. Access to personal email accounts using the City computers and the Internet during lunch and/or breaks or for emergencies may be permitted. However, personal use of the City's IT systems is at the user's own risk and may be accessed, reviewed, copied, deleted or disclosed by the City.

6.5. The following uses of the City's IT systems are prohibited:

6.5.1. Usage for private gain, or in connection with compensated outside work, game playing, stock trading, browsing social media sites or chat rooms;

6.5.2. Political or religious activities; activities or messages that are illegal or in conflict with local, state, or federal law; applicable regulations of the network being used; City policies, or procedures;

6.5.3. Unauthorized attempts to access data or break into any City or non-City system, and theft or unauthorized copying of electronic files or data;

6.5.4. Harmful activities such as creating or propagating viruses; disrupting services; damaging files; and intentionally destroying or damaging equipment, software, or data belonging to the City.

6.6. All messages from the City's IT systems must appropriately identify the sender. IT 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 or the owner of that email

account. No previously sent e-mail message shall be changed without authorization from the original author.

6.7. Unless specifically authorized, no postings may be made to any social media sites in the City's name. (Please refer to the City's AR 509 Social Media Policy for Elected and Appointed Officials and 510 Citywide Social Media Policy and consult with the Office of Communications).

6.8. Intellectual property (including but not limited to computer software, movies, books and music) is protected by copyright. It is not to be copied from, into, or by using City-computing facilities, except as permitted by law or by the contract with the copyright owner. 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 IS Department staff.

6.9. Access to City's IT systems equipment and resources by recognized employee organizations/bargaining unit is allowed consistent with this policy and any provisions in an applicable Memorandum of Understanding. Access shall be authorized only to the extent that bargaining unit 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 their representatives shall have no greater access to the use of computer resources than employees of the City. The use of City IT systems to communicate between bargaining unit representatives and City representatives is considered city business and shall be allowed during regular business hours.

6.10. Authorized Users shall ensure that all IT devices 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 IT devices shall be maintained by the user that they are issued to. IT devices and ancillary equipment must never be left unattended in locations such as airports and hotel lobbies. Whenever practical, IT devices shall be secured with the supplied security device(s) and other security measures such as log-in passwords.

6.11. Authorized Users are expected to report unauthorized access, including unauthorized access attempts or other improper usage of IT devices, or other information processing equipment. If a user becomes aware of a potential abuse, policy violation or cyber security concerns the user must take immediate steps as necessary to ensure the safety and security of information resources by contacting their immediate supervisor and/or the IS Department.

6.12. For security reasons, the City only permits the use of Microsoft Teams for instant messaging (IM). Other IM or chatting applications may not be used on City computers.

6.13. City officials and personnel in possession of confidential information shall take all reasonable and necessary steps to protect the confidentiality of the information and minimize the likelihood of inadvertent transmission of the information to unintended recipients. City officials and personnel must exercise caution when creating or transmitting city business information electronically. Confidential information may not be transmitted to other city officials or personnel who are not authorized to receive such information. E-mail which contains confidential attorney-client privileged information may not be disclosed, except by the City Attorney's Office, unless so authorized by the City Manager or designee, or as required under

law. If a user is unsure as to whether a communication is authorized, it is the user's responsibility to inquire with their supervisor or the City Attorney as appropriate.

6.14. It is personnel's responsibility to ensure confidential information shared with an external party requires a form of authentication. IS Department should be contacted if assistance selecting a suitable method is required.

6.15. Remote access to the City's network provided to personnel may be allowed by their respective Department Head and strictly for business-related purposes, not to be shared with any individuals who are not employed/authorized by the City.

6.16. Computers should be locked, either manually each time personnel leave their desks for any period of time, or automatically using a password-protected screen saver. At the end of the workday, employees shall sign-out of their computer. The computer is to be left on, running over night to receive software updates. IS Department staff may ask users to change their passwords temporarily to perform installations, diagnostics, repairs, replacements, upgrades, or maintenance. Once completed, personnel shall immediately change their password to something unique and secure. (Please refer to AR 608 for more information about cyber security and password protections).

6.17. When an employee or on-site contractor requires access to a City computing resource, the department in which the employee resides, completes and submit the *Network User Security Account form* (Attachment 2) on the Surfnet Forms & Templates section via requesting department's assigned representative (the City's Laserfich application account required).

6.18. When an employee or authorized user is separated from the City, all application and computer accounts should be disabled immediately by the IS Department.

6.18.1. Each employee's personal folder and mailbox data will be retained for two years.

6.18.2. Their supervisor may request read-only access to this data for City business purpose only. Access to the data will be granted for three months by default. Data that should be retained should be copied to an alternate location.

6.18.3. Email of separated employees will not be forwarded to other employees, supervisors or shared mailboxes. An automatic email reply can be set informing senders of an alternate contact.

7. Procurement & Installation:

7.1. No IT devices or software is to be purchased without the review and approval of the IS Department.

7.2. No personally owned IT devices or software is to be used with or installed on any city computer resource without the review and approval of the Information Services Department.

7.3. Procurement of any IT devices or software shall be procured by creating a ticket for the IS Help Desk with the exception of printers. The Finance Department approves and processes the

procurement of printers. With the exception of IS staff, City-issued CalCard/credit cards, or petty cash shall not be used to purchase IT devices.

7.4. IT consumable items such as toner cartridges, CDs, DVDs, flash drives, and paper, do not require IS 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.

Distribution:

All employees may access the Administrative Regulations via the SurfNet or City website: www.huntingtonbeachca.gov/AR.

Attachments

1. AR 605 Computing Resource Use Policy Agreement Declaration Form
2. Network User Security Account Form (hyperlinked in SurfNet – Forms & Templates – IS)

John Dankha, Chief Information Officer
Information Services Department

Approved As to Form
Michael Gates, City Attorney

Eric G. Parra
Interim City Manager

Review Schedule

REVIEW DATE	DEPT. HEAD INITIAL	CITY MANAGER SIGNATURE

ADMINISTRATIVE REGULATION
Office of the City Manager

City of Huntington Beach
AR 605 Computing Resource Use
Policy Agreement Declaration

DECLARATION BY THE EMPLOYEE:

The undersigned employee declares that:

a. He/she has been given the time needed to read and has, in fact, read the Computing Resource Use Policy in full;

b. An authorized City representative has offered to provide him/her, if so required, with information and explanations pertaining to this Policy;

c. Each and every one of the provisions of this Policy is legible;

d. An authorized City representative has given the employee a copy of this Policy.

EMPLOYEE'S COMMITMENT

The undersigned employee, as an authorized user, commits and agrees to:

a. Follow all provisions of this Policy;

b. Promote the spirit and the letter of this Policy;

c. Become familiar on a regular basis with any revisions or amendments to this Policy, as soon as the revised or amended Policy is made public, via posting on Surfnet or e-mail, and follow all provisions of the revised or amended Policy.

ACKNOWLEDGMENT

I have read the Computing Resource Use Policy (AR 605) and understand its provisions. I understand that use of the City's computer system, in any capacity, is a privilege and not a right. I understand that I have absolutely no right to privacy in any of the City's computer systems, ID's, files, etc., and that any materials that I have created, saved, downloaded, erased, etc., are subject to search and review by my employer. I accept responsibility for the appropriate use of City computer resources, including all computer systems, network systems, Internet, and Intranet web sites, or other data processing equipment owned by the City, as well as remote computers or computer systems when used to access the City computer resources as outlined in the Computing Resource Use Policy. I understand that use of City computer resources in violation of the Computing Resource Use Policy may result in employee discipline and/or the cancellation or restriction of user privileges. I agree to report any use, which is in violation of the Computing Resource Use Policy, to Information Services or to management.

THIS SECTION TO BE COMPLETED BY THE EMPLOYEE			
Agreement to the above:			
Employee's Name ***(Print)***	Signature	Phone	Date