City of Richmond
Administrative Manual

SUBJECT: Use of Technology Policy
[formerly E-mail (Electronic Mail) Policy]

SECTION: Information Technology **POLICY NUMBER:** AP 655

INITIAL DATE PREPARED: August 25, 1999 **LAST DATE REVISED:** January 28, 2015

I. PURPOSE

To assure that all, temporary or permanent employees, interns, volunteers, agents (including consultants, vendors and other contract workers), elected officials and other individuals with authorization to use ("Users") the City of Richmond's ("City") computer systems and/or related technologies are aware of and observe specific policies and procedures when operating City computer equipment and systems.

II. POLICY

It is the policy of the City to promote efficient and proper use of all City's communication technologies, including but not limited to the City's email system, workflow, data storage, business application systems, hardware (including connected and disconnected computers, servers, switches, routers, etc.), software, email, access to the Internet, Intranet, World Wide Web, voicemail, and data thereon (hereafter "City's Computer Systems") regardless of physical location or the form in which they are maintained. City's Computer Systems are to be used for City business in the course of normal operations.

Users who use the City's Computer Systems do so with no right to or expectation of privacy or confidentiality.

Violations of this administrative policy subject employees to discipline up to and including termination. In the event of a policy violation, the City may pursue all remedies provided under the law, including advising legal and/or law enforcement authorities of any violation of law.

The City reserves the right to change these policies and procedures at any time.

III. PROCEDURE

A. ACCESS

Unauthorized access to computer technologies, including but not limited to, equipment, software, and systems by unauthorized Users is a violation of City policy and grounds for disciplinary action. Unauthorized access to City computer equipment, software, and systems by the public may be illegal. Accessing City's

Computer Systems is regulated in accordance with AP 653.

The City email service is intended for internal use by City employees. Access shall be password protected. Assignment and installation shall be done only by City Information Technology (IT) department staff. Third parties will not be given access to the City email system.

Users will comply with license agreements and policies of systems administration and on-line services made available by the City. Users will comply with copyrights, intellectual property rights, and contracts.

Users will maintain hardware and software as installed by IT and not make unauthorized changes.

The City recognizes that under certain circumstances, employees may seek to access City computer systems including but not limited to voicemail or emails to engage in work-related activities outside their regularly scheduled hours. Employees must first obtain authorization from their supervisor before performing any such work. **Employees who choose to access City-owned voicemail or email accounts during non-working hours do so with the understanding that these activities are neither required nor expected**.

B. USAGE

EMAIL

City employees shall use the electronic mail system only for City related activities. Email shall not be used for solicitations, personal messages or to disseminate sensitive information.

Unauthorized accessing of email (electronic snooping) by any employee is a violation of City policy and may be a violation of state and federal law.

Users may not transmit, obtain or access information in violation of any federal, state or local law including copyright laws and/or transmit, obtain, or access files or communication for any unlawful purposes.

WEB/INTERNET

The Internet shall be used for City-related business only. Web resources are made available to City Users to improve communication and to provide information related to City business. As the Internet is a global electronic information infrastructure of networks used by educators, businesses, governments and individuals, certain restrictions are necessary to avoid inappropriate use, and

possible adverse public perceptions. City information network resources shall not be used for illegal, harassing, libelous, obscene or other purposes, which could expose the City to liability.

SOCIAL NETWORKING POLICY (See AP-655.1)

The City recognizes that Social Networking (such as personal websites, blogs, social communications, online group discussions, text messaging, message boards, chat rooms, etc.) are used by many Users. The City respects the right of Users to maintain a blog or post a comment on social networking sites. The City is committed to maintaining its identity, integrity, and reputation. The City has a legitimate public interest in protecting its logo, City name, and other intellectual property, and in making sure that its employees do not violate criminal or civil law, or privacy rights.

APPROPRIATE USE:

Email, Intranet/Internet and related services made available to Users shall be used primarily for City business. Incidental and minimal personal use is allowable to the extent that the use does not fall within one of the categories listed under prohibited uses and does not hinder a User's ability to effectively and efficiently accomplish his or her job functions.

PROHIBITED USES ON CITY NETWORKS AND EQUIPMENT:

Below are examples of prohibited uses:

- Use in violation of local, state, and/or federal law.
- Use to commit fraud or steal data, equipment or intellectual property.
- Use the network for an illegal activity including violation of copyrights, license agreements or other contracts.
- Use for any for-profit activities unless specific to the City's charter, mission, or duties, and with express authorization from the IT Director or his/her designee
- Use for fundraising or public relations activities not specifically related to City activities.
- Use for private business, including commercial advertising.
- Use to access or distribute indecent or obscene material.
- Use to access any pornographic sites.
- Use for sending, downloading, displaying, printing or otherwise disseminating material that is sexually explicit, profane, obscene,

harassing, fraudulent, racially offensive, defamatory, libelous, discriminatory based on race, national origin, sex, sexual orientation, age, disability or religious or political beliefs, or which is otherwise unlawful.

- Use for religious or political causes.
- Use for threats, harassment, slander, defamation, obscene or suggestive messages or offensive graphical images.
- Use for Political endorsements.
- Use Internet services that interfere with or disrupt network users, services, or equipment.
- Seek out information on, obtain copies of, or modify files and other data which is private, confidential or not open to public inspection or release (as set forth in Government Code or City's Municipal Code) unless specifically authorized to do so once the legal conditions for release are satisfied.
- Copy any software, electronic file, program or data using Internet services without a prior, good faith determination that such copying is, in fact, permissible. Any efforts to obtain permission should be adequately documented.
- Seek information on, obtain copies of, or modify files or data belonging to others without authorization of the file owner. Seeking passwords of others or the exchanging of passwords is specifically prohibited.
- Intentionally representing oneself electronically as another user, either on the Intranet or elsewhere on the Internet. Users shall not circumvent established policies defining eligibility for access to information or systems.
- Post on a blog or social networking site during their working time or at any time using City equipment or property. However, employees are authorized to post on the City's website if the post relates to employees' wages, benefits, working conditions, or terms and conditions of employment with the City. If an employee identifies himself or herself as an employee of the City on any social networking site, the communication must include a disclaimer that the views expressed are those of the author and do not necessarily reflect the views of the City.
- All City policies and rules regarding confidential information apply in full to blogs and social networking sites.
- Users are prohibited from misappropriating or using without permission the City's logo and City intellectual property on any social networking site or other online forum. Users are reminded that there are civil and

criminal penalties for posting copyrighted material without authorization.

C. RECORD RETENTION

All email messages are considered City property. The Information Technology Department will include e-mail messages in their routine data back-up process, as well as archive email messages after 90 days. All emails are archived regardless of retention schedules.

D. MANAGEMENT

The City will not monitor electronic email messages as a routine matter. However, the City Attorney or his/her designee may review email communications in response to public records act requests, discovery requests or to determine possible violations of City policy. The City reserves the right to access and disclose the contents of employee email messages but will access only when it has a legitimate business need to do so.

E. DISCLOSURE

The City reserves the right to disclose any computer usage that violates this policy to law enforcement officials without any prior notice to any employees.

The City reserves the right to monitor public blogs and public social networking forums for the purpose of protecting its interests and maintaining compliance with this policy.

F. REMOTE ACCESS

1. The City offers its employees the ability to access their applications, documents and email from home or other remote locations using non-City computers and Internet access accounts. This service will allow employees to check their email, calendar, contact list, and other files/systems from their home or other computer. This access is provided through the use of VPN and SSL technologies. Employees who use this service must adhere to the guidelines set forth in this document.

2. The City offers this service as a convenience to employees and does not require employees to use this service. **As such, employees shall not be compensated for time spent accessing their City applications, documents or email through this service without express prior authorization. Authorization for overtime**

compensation must be approved in advance by a Department Head or authorized supervisor. See the appropriate section in your bargaining unit's MOU for instructions on overtime approval or contact the Human Resources Department.

3. Because the City offers remote access as an optional service, the City cannot provide technical support to employees for their home computers. Every effort will be made to provide employees with the requirements and instructions necessary to utilize this service.

4. Employees who use this service do so at their own risk and the City will not be held liable for damage to employees' home computers.

5. Use of this service should be for work-related purposes only.

6. Passwords are to be kept confidential and they should not be stored on any computer including employees' home computers.

7. Employees using this service should take reasonable precautions to prevent computer viruses from infecting the City's network. These precautions include, but are not be limited to, using anti-virus software and keeping it current with virus definition updates.

8. Personal computers and other electronic devices (cell phones, pda's, etc.) may not be connected directly to the City's trusted LAN network. All access to the trusted LAN network segment for these devices will be through a VPN using two factor strong authentication meeting Federal Information Processing Standard (FIPS) 140-2 requirements.