Acceptable Use of Information Technology
Administrative Policy #1

September 2019

I. POLICY

The city's Acceptable Use Policy does not impose restrictions that are contrary to the city's established culture of openness, trust, and integrity. The city is committed to protecting its constituents and employees from illegal or damaging actions by individuals, whether those actions are known or unknown to the city. Inappropriate use exposes the city to risks, compromise of network systems, illicit use of network systems, data, and services, and legal liability, and may result in disciplinary action under the city's Standards of Conduct and/or legal prosecution. This Policy is not intended to restrict communications or actions protected or required by federal, state, or local law.

II. APPLICABILITY

The purpose of this Policy is to establish guidelines for the acceptable use of information technology, which for purposes of this Policy includes but is not limited to the city's computer equipment, cellular phones, personal digital assistants (PDAs), network resources, electronic mail (email), text messages, the internet, network connectivity, storage repositories, and other electronic information equipment and systems.

All employees, contractors, consultants, business associates, vendors, temporary employees, interns/externs, and other city workers, including all personnel affiliated with third parties ("Authorized Users") are required to comply with city policies and local, state, and federal laws, and maintain responsibility for using these resources in an appropriate, ethical, and lawful manner.

III. USER PRIVACY

No city employee, or individual representing the city's interests or conducting business, who is authorized to access city technology shall have any expectation of privacy in city technology, electronic records, web pages, mobile communications, or web sites that are created; visited; manipulated; stored; receive; transmitted or retrieved in, by, or through any city technology; with the exception that any electronic records and other communications in the course of city business which are protected by the attorney-client privilege or the attorney work-product doctrine created, sent, or received by, or at the behest or under the oversite of, the City Attorney's Office or outside counsel retained by the city, shall remain strictly confidential. In order to access, retrieve, or copy any city technology or electronic records, city employees shall have no expectation of privacy in a city-supplied vehicle, city office, cubicle, or other city workspace, and the furniture contained therein, which may be entered, inspected, and searched for this purpose. However, no personal items such as purses, briefcases, clothing, or bags may be searched.

A. Monitoring

The city may, without notice, audit, monitor, inspect, copy, and retrieve, any city technology or technology connected through external secure access, and any electronic record, or user activity on city-approved mobile and fixed devices, including but not limited to email, messages, files, inbound and outbound file transfers, web sites visited, including uniform resource locator (URL) of pages retrieved, and the date, time, and user associated with each use. This monitoring may occur at any time without notice and without the user's awareness or permission. Internet traffic over city information systems shall be proxied and inspected for malicious code or inappropriate content prior to delivery to the user. Filters shall track user internet activity, and be monitored for violations of this policy, as well as any other applicable laws, regulations, and city policies and procedures. Such activity is for the performance of legitimate city business including but not limited to the following:

1. To monitor and evaluate the efficiency, quality, use, and volume of city services, and city technology, and to evaluate the achievement of service goals.

2. To investigate suspected violations of law or city or departmental policies by city employees or third parties, when deemed necessary or appropriate.

3. To audit or monitor networks that connect to the internet or other publicly available networks to support identification and termination of unauthorized or improper activity.

4. To comply with a law, court order, or another legitimate governmental purpose.

B. Personal Electronic Records

Storage of user's personal information on city information systems is done at the user's risk. Such information may be subject to public disclosure or review by city officials. By using any city information system, the user agrees to surrender any data contained in such information system whether the data is owned by the city or alleged to be owned by anyone other than the city.

C. Internet Monitoring

The Department of Information Technology (DIT) shall monitor internet uses from all computers and devices connected to the city's network. For all traffic, the monitoring system records the source IP Address, MAC Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Log records are subject to inspection and audit at any time for work-related purposes or to determine whether violations of city policies or laws have occurred.

IV. INFORMATION SYSTEM SECURITY

Users shall respect the confidentiality and integrity of any city information system, be familiar with city information-system security policies and procedures and report any security weaknesses or breaches in city information systems to DIT. Users shall respect security controls for city information systems and not attempt to or circumvent those controls. Users shall not access or attempt to access any city information system without authorization from DIT or department director. Users shall refrain from activities that intentionally or inadvertently disrupt, impair, or undermine the performance of city information systems.

Users shall refrain from divulging to unauthorized persons any details regarding city information systems or architecture unless authorized by the DIT. The use of strong passwords to access city information systems and city-approved mobile communications devices is for the protection of the city, and not any user.

Users shall prevent the disclosure of their USERID, PASSWORDS, security tokens, or other similar information to unauthorized users. Also, using another person's credentials, files, systems, or data without permission is prohibited. Users are responsible for all activities which transpire under their USERID.

Network Users shall be required to complete semi-annual security awareness training through appropriately defined mediums. Failure to complete assigned training within the required time frame will result network access deactivation.

V. DEFINITIONS

A. City Technology

All information technology resources, including but not limited to computer networks (including email, intranet, internet, etc.), hardware, software, systems, programs, and devices (including cell phones, personal digital assistants, tablets, pagers, storage media, etc.) supplied, owned, or operated by or for the city of Portsmouth for use in city business. City technology includes all such information technology resources of the city's contractors and Third-Party Service Providers which are provided to city employees for use in city business.

B. Device

Any device that is capable of receiving or transmitting city data to or from city information systems.

C. Electronic Records

Consist of computer records and files, emails, text messages, voice messages, images, web pages, logs, audio and visual recordings, and optically scanned records, also known as machine-readable records, that are created, viewed, manipulated, stored, retained, sent, or received, by electronic means in, by, or

through city technology. Most Electronic Records are also Public Records under the Virginia Freedom of Information Act and the Virginia Public Records Act and are referred to as Electronic Public Records.

D. Information

Any and all data, regardless of form, that is created, contained in, or processed by, information systems facilities, communications networks or storage media.

E. Information Systems

Any and all computer-related equipment and components involving devices capable of managing, transmitting, receiving or storing information or data including, but not limited to, a USB drive, CD-R, laptop or personal computer, personal digital assistant (PDA), cell phone, handheld computer, internal hard drive, external hard drive, flash storage, hosted or cloud storage, servers and computer printouts. Additionally, the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to create, collect, record, process, store, retrieve, display and transmit information.

F. Internet

A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and educational institutions.

G. Intranet

A private network for communications and sharing of information that, like the internet, is based on TCP/IP, but is accessible only to authorized users within an organization.

H. Password

A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data. A strong password is one that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, Social Security number, etc.

I. Server

A server is a system that provides services to client systems. The computer that a server program runs in is also frequently referred to as a server (though it may contain several servers and client programs).

J. Third-Party Service Providers

Firms that provide services to all or some city employees for use in city business including but not limited to services for the creation, transmission, retrieval, use, or storage of electronic records, including providers of cellular phone service, internet service, message service, and other data and voice transmission services. A Third-Party Service Provider may, but is not required to be, under contract with the city.

K. User

An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

L. Web Page

A document on the World Wide Web (www). Every webpage is identified by a unique Uniform Resource Locator (URL).

M. Website

A location on the World Wide Web (www), accessed by typing its address (URL) into a web browser. A website always includes a home page and may contain additional documents or pages.

VI. ACCEPTABLE USE OF INFORMATION TECHNOLOGY

A. All technology equipment purchases are to be approved by the Department of Information Technology (DIT) or an authorized agent of the Department.

B. The installation, relocation, upgrade, or disposal of IT equipment must be approved and performed by the Department of Information Technology or an authorized agent of the Department.

C. Connecting of privately-owned electronic devices, including portable hard drives, to the city's network are prohibited without the prior approval of the Department of Information Technology.

D. IT equipment is provided for city business. The excessive use or permitting another's excessive use of city computer or network assets, as determined by the City Manager, Chief Information Officer or Department Head, for private or personal purposes may result in disciplinary action under the city's Standards of Conduct.

E. Software License and Usage

1. The purchase and installation of all software must be approved and performed by the Department of Information Technology or an authorized agent of the Department.

2. All software must be properly licensed for use on city equipment. Employees are expected to comply with the terms and conditions of the software licensing agreement. The installation of unlicensed and unapproved software is prohibited and may be a violation of Federal copyright laws. Any software installed without a license or proof of purchase must be removed.

3. Downloading of unlicensed or protected software programs or files from the Internet or other non-city IT resources is prohibited, these may include but are not limited to photographs, movies, music or commercially developed software.

4. The creation, modification, programmed or knowledge leading to the creation of software or related systems shall be the property of the city of Portsmouth with all rights and trademarks associated.

5. The installation of software or hardware pertaining to city information systems on infrastructure not directly controlled or affiliated with the city shall be prohibited, unless approved by City Manager, City Attorney, and Chief Information Officer.

F. Information Handling and Storage

1. Employees are to store all city-related electronic information and data on the city's network file servers and not on the local drive of a desktop or laptop computer. The Department of Information Technology provides for the backup of information stored on the network servers. Responsibility for the backup and security of files on the local disk of a desktop or laptop computer lies with the employee. The use of non-city owned data hosting and business application providers on the internet must be approved by the Department of Information Technology.

2. You must properly handle, store, and securely dispose of city information in accordance with the Library of Virginia records retention schedules. You are responsible for any confidential or highly confidential information that you access or store. Do not allow others to view, access, or otherwise use any confidential or highly confidential information you control unless they have a specific business need to know.

3. Employees should use care when storing any information on flash drives, CDs, or other portable media. Physically secure any media containing city information, including hard drives, CDs, disks, paper, voice recordings, removable drives (e.g., thumb drives, flash drives, USB drives), or other media. Confidential, highly confidential, and other sensitive information should not be stored on portable media unless there is an absolute business need. Portable media containing confidential, highly confidential, or other sensitive information must be stored in a locked area when not in use.

    a. Shred or otherwise destroy paper that contains Confidential or Highly Confidential Information prior to disposal. Return all electronic, magnetic, or optical media to the Department of Information Technology for secure disposal when it is no longer required to meet business needs.

    b. Portable storage devices require approval from Chief Information Officer or designee.

    c. All files and data stored on city equipment and media are the property of the city of Portsmouth. The city reserves the right to access these files at any time and without prior notice.

G. Internet Use

Employees are responsible for using the internet in an appropriate, ethical, and legal manner. Inappropriate and/or unauthorized use will result in revocation of the privilege and may result in disciplinary action under the city's Employee Standards of Conduct. Limited, occasional use for personal, non-business purposes is acceptable as determined by the City Manager, the City Manager's designee, or Department Head, provided it does not adversely affect the performance of the employee's duties, does not negatively impact the information systems' resources, integrity, or ability to appropriate conduct city business and does not violate city policies or any federal, state, or local laws.

The Department of Information Technology shall block access to internet websites and protocols that are deemed inappropriate for the city's corporate environment. The following protocols and categories of websites will be blocked, and the following does not represent the entire filtering category:

1. Adult/Sexually Explicit Material
2. Advertisements & Pop-Ups
3. Chat and Instant Messaging
4. Gambling
5. Hacking
6. Illegal Drugs
7. Intimate Apparel and Swimwear
8. Peer to Peer File Sharing
9. Personals and Dating
10. Social Network Services
11. SPAM, Phishing and Fraud
12. Spyware
13. Tasteless and Offensive Content
14. Violence, Intolerance, and Hate
15. Web-Based Email
16. Storage Repository

H. Desktop, Laptop, and End-User Controls

You may only access the city's network using approved end-user devices that support the city's current minimum information security standards. Standards for end-user devices may include protective controls and specific configurations, such as anti-virus software, patching levels, and required operating system or other software versions. The city-owned devices may be configured to automatically receive upgrades. You may be denied remote access using non-city owned devices that do not meet current standards.

You may only use your own city-provided account(s) to access the city's network and systems unless you have been specifically authorized to use a device-specific, administrative, or other account. Screen saver passwords, also known as "workstation timeouts" or "lock screens," secure confidential information by protecting active computer sessions when you step away. Locking screen savers must activate after a maximum inactivity time of 15 minutes. If you handle highly confidential information, lock your screen any time you leave it unattended.

I. Cloud Computing

The city may use internet-based, outsourced services for some computing and data storage activities based on business needs. Cloud computing services store data and provide services in internet-accessible data centers that may be located almost anywhere. Cloud services vary significantly in-service levels and security provided.

While cloud services may offer an attractive cost model, they also present significant risks. Using them may also affect the city's ability to comply with some laws. Before using any cloud computing services to collect, create, store, or otherwise manage the city's confidential or highly confidential information, you must obtain approval from the City Attorney and the Chief Information Officer.

J. Remote Access

Remote access to city information systems shall only be permissible through the Department of Information Technology provided and supported remote access software applications, protocols, delivery mechanisms, and if necessary, Department of Information Technology provided and supported anti-virus software. Remote access for employees shall be requested by a Department Head and approved by the Chief Information Officer or designee after a determination has been made that access is required to perform assigned duties, or the user is defined as "essential" personnel by the city.

K. Theft, Loss, Unauthorized Disclosure

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of city proprietary information, computers, removable storage, or other electronic or non-electronic devices.

VII. USE OF ELECTRONIC MESSAGING

City users are responsible for the content of all text, audio-video or images stored or transmitted over the city's electronic messaging (i.e., email) and other collaboration systems, such as instant messaging. All messages communicated on city email systems shall contain the sender's name. Email or other electronic communications shall not be sent on city email systems which mask or attempt to mask the identity of the sender. Users shall make reasonable efforts to validate the authenticity of emails received prior to opening any attachments or clicking on links. The following activities are examples of acceptable uses of city email systems:

A. Communicating and exchanging information directly related to the mission, charter, or work tasks of the city;

B. Communicating and exchanging information for professional development, to maintain the currency of training or education, or to discuss issues related to the city business;

C. Applying for or administering grants or contracts for city research or programs;

D. Conducting advisory, standards, research, analysis, and professional society activities related to the city business;

E. Announcing new laws, procedures, policies, rules, services, programs, information, or activities;

F. Incidental personal use; users of city email systems shall not give the impression in their communications to persons receiving such emails that they are representing, giving opinions, or otherwise making statements on behalf of the city or any agency of the city, unless otherwise authorized to do so. Where appropriate, a disclaimer shall be included such as, "The opinions expressed are my own, and not those of

city of Portsmouth," unless it is clear from the context that the email's author or sender is not representing the city.

VIII. PROHIBITED USE OF INFORMATION TECHNOLOGY

A. Certain activities are prohibited when using city information systems, applications, data, and resources, whether on city-owned or personally-owned devices, except when the Department of Information Technology and Departmental Heads have determined such activities are necessary for the performance of a user's official duties. The city prohibits use of its resources to engage in activities such as (but not necessarily limited to) the following:

1. Any activity that violates or encourages others to violate the city's Standards of Conduct and/or city policies.
2. Any activity that causes harm to individuals or damage to the property of others, i.e., attacking someone through slander.
3. Using "taglines" in any city technology or electronic public record. Taglines are usually phrases, catchwords, slogans, or quotations, which are sometimes added at the end of an email or other written communication, which become identified or associated with a person, group, service, product, etc. Only city or department approved taglines may be included in city technology and electronic public records. (Note: This prohibition also applies to all non-electronic public records created or sent by city employees in the course of city business.)
4. Creating or propagating viruses or disrupting services;
5. Transmitting, disseminating, or otherwise providing access to all levels of confidential information;
6. Manipulating, damaging, deleting, or destroying city equipment and electronic information;
7. Decoding or attempting to decode passwords or encrypted information, or to otherwise circumvent system access control or other security measures;
8. Gaining or attempting to gain unauthorized access to others' networks or systems, including another user's credentials for city systems;
9. Revealing your account password to others or allowing the use of your account by others, including family and other household members;
10. Altering city-provided access configurations without specific written authorization by the Chief Information Officer;
11. Using city resources for partisan political purposes, including the use of email to circulate advertising or other material for candidates;
12. Making or using illegal copies of copyright-protected material (including software), storing such copies on city equipment and electronic information or elsewhere, transmitting the same through city equipment and electronic information, or downloading, storing, or distributing materials in violation of another's copyright;

13. Installing or distributing unlicensed or pirated software;
14. Misusing or wasting IT resources by intentionally placing a program in an endless loop, excessive printing, misuse of processing capabilities, or any other waste of city IT resources;
15. Disconnecting or moving, without consent, city electronic information or any stationery item of city equipment;
16. Broadcasting unsolicited or fraudulent messages or emails;
17. Hacking, spoofing, or launching denial of service attacks;
18. Creating or transmitting false or malicious information;
19. Distributing or attempting to distribute malicious software (malware);
20. Spying or attempting to install spyware or other unauthorized monitoring or surveillance tools;
21. Committing criminal acts such as terrorism, fraud, or identity theft;
22. Downloading, storing, or distributing child pornography or other obscene materials;
23. Using encryption or other technologies to hide illegal, unethical, or otherwise inappropriate activities;
24. Creating undue security risks or negatively impacting the performance of the city's network and systems;
25. Causing embarrassment, loss of reputation, or other harm to the city;
26. Intentionally uploading, disseminating, accessing, viewing, downloading, posting, transmitting, or printing information or material that is abusive, offensive, sexually explicit, harassing, implies violence, or discriminates on the basis of race, sex, color, religion, national origin, age, disability, or any other basis prohibited by law (however, the City Manager, Director of Human Resource Management, or the Chief Information Officer may grant authorized employees access to such information for investigation and/or law enforcement purposes);
27. Harassing or intimidating other persons;
28. Distributing joke, chain letter, commercial solicitations, or hoax emails or other messages (spamming);
29. Using the city's network, resources, equipment, or electronic information for personal gain (e.g., cryptomining or selling processing power) or gambling;
30. Disrupting the workplace environment, creating a hostile workplace, or invading the privacy of others; and
31. Providing information about, or lists of, city employees or constituents to parties outside the city.
32. Using internet peer-to-peer file sharing services.
33. Using internet-based remote access services to access the city's network or systems without prior approval. See the Remote Access section of the Policy for additional guidance.

B. Circumventing Security Controls

The city may treat any attempt to bypass or circumvent security controls as a violation of this Policy. For example, sharing passwords, deactivating anti-virus software, removing or modifying secure configurations, or creating unauthorized network connections are prohibited.

C. Illegal Activities

Do not use the city's network or systems for activities that may be deemed illegal under applicable federal, state, local, or international law. If the city suspects illegal activities, it may report them to the appropriate authorities and aid in any investigation or prosecution of the individuals involved.

IX. CONFIDENTIALITY

Users shall comply with all laws, regulations, and city policies and procedures prohibiting or limiting the disclosure of confidential information, including but not limited to, personal information (e.g. medical records, financial information, and social security numbers), tax information (e.g. information of any person firm or business with respect to any transactions, real and personal property, income or business of the taxpayer) and city employee personal information (e.g. medical records, financial information, and social security numbers). Confidential information transmitted on city information systems shall be sent only to those recipients who are authorized to receive such confidential information. Users shall take all steps necessary to protect the privacy of confidential information maintained by the city from unauthorized access. These measures include but are not limited to, enabling password protection on any fixed or mobile system, or otherwise locking and closing computer screens when leaving even for brief period, and logging off or terminating a system session when access is no longer needed, or the user is leaving for the day. Users shall follow all Federal, Commonwealth, and city policies and guidelines defining data classification and protection requirements.

X. TERMINATION OF ACCESS

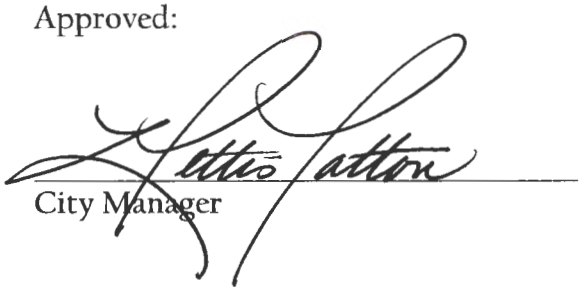
Engaging in prohibited uses of the city's information systems shall be considered a violation of city policy and may result in disciplinary action in accordance with city policy. The city reserves the right to deny further access to its information systems when such action is necessary to protect system security and performance. If deemed necessary by the Department Head, Chief Information Officer and the Director of Human Resource Management, any user's access to city information systems and all city devices shall be terminated, and the user shall return to the Department of Information Technology all city-owned mobile communications devices issued. Access privileges to city information systems through a non-city issued device shall be terminated for any reason deemed necessary by IT to protect the city.

In addition, upon separation from the city, user access to city information systems and all city devices shall be terminated. The user shall return to the department or Department of Information Technology all city-owned communications devices issued.

Anyone who suspects a user of any inappropriate use of city information systems should direct questions concerning any inappropriate use to their supervisor, the Department of Human Resource Management, or Department of Information Technology.

If you have any questions regarding acceptable use of city's information technology, please contact the Department of Information Technology at (757) 393-8871 and for disciplinary matters, contact the Department of Human Resource Management at (757) 393-8626.

Approved:



City Manager