CITY OF PORTSMOUTH

ADMINISTRATIVE POLICY

#1

August 2010

SUBJECT: Information Technology Acceptable Use Policy.

PURPOSE: 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 (PDA), network resources, electronic mail (E-mail), text messages, the Internet and other electronic information equipment and systems. All employees are required to comply with City policies, local, State and Federal laws and maintain responsibility for using these resources in an appropriate, ethical and lawful manner. Inappropriate use may result in disciplinary action under the City's Standards of Conduct and/or legal prosecution.

If you need any assistance or have questions concerning any of the procedures in this policy or need technical assistance, 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.

I. INFORMATION TECHNOLOGY USAGE

This policy provides guidelines for the use of Information Technology (IT) equipment, software and data. IT resources are provided to city employees for use in the performance of city business. All City IT equipment, software and data are the property of the City of Portsmouth, Virginia. Public electronic records are subject to disclosure in accordance with the Virginia Freedom of Information Act (FOIA).

A. Information Technology Equipment Use

(1) All computer and network equipment purchases are to be approved by the Department of Information Technology or an authorized agent of the Department.

(2) 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.

(3) 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.

(4) 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 or Department Head, for private or personal purposes may result in disciplinary action under the City's Employee Standards of Conduct.

B. 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.

C. Data / File Storage

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. Employees should use care when storing any information on flash drives, CDs or other portable media and should not store any sensitive information on them. The use of non-City owned data hosting and business application providers on the Internet must be approved by an employee's Department Head and the Department of Information Technology.

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.

II. ELECTRONIC MAIL (EMAIL)

This policy provides guidelines for the use of the City Electronic Mail (E-mail) system. Use of the City's E-mail system is intended for official City business. Each department is responsible for ensuring business-related use in an appropriate and legal manner.

Access to E-mail is established by the Department of Information Technology upon approval of an employee's Department Head. Department Heads are responsible for notifying the Department of Information Technology when an employee's Email account is to be terminated or an employee relocates (refer to Section IV.B. for more information).

A. Email Use

The City's E-mail system may not be used to compose, send or forward information that could be deemed offensive, disruptive, violent, harassing, sexually explicit or discriminatory against others based on race, sex, color, religion, national origin, age or disability.

To compose, send or forward such information, whether in text, image or audio content, is a violation of laws and City policies, including the City's Employee Standards of Conduct. Employees are responsible for the content of messages they compose or send.

All messages composed, sent and received are the property of the City of Portsmouth and are subject to City monitoring. The City reserves the right to access and disclose messages, files or records of any kind at any time that are stored, sent or received on City equipment. Electronic documents, including E-mail, are subject to disclosure under the Virginia Freedom of Information Act. They may be used for disciplinary action, grievances and other administrative procedures, as well as subpoenaed for use in legal proceedings.

Limited, occasional use for personal, non-business purposes is acceptable as determined by the City Manager, 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 system's resources, integrity, or ability to appropriately conduct City business. Limited personal use by employees shall comply with the City's Employee Standards of Conduct, departmental policy, and Federal, State, or local law.

B. E-mail Retention

The E-Mail system is not to be considered a long-term document storage system. E-Mail may be retained in the system for up to 12 months. The State Library of Virginia provides guidelines for public record retention. E-Mail users are to determine if the content of the E-Mail requires it to be retained by Virginia Records Retention laws. It is the employee's responsibility to retain E-Mails in accordance with the State Library of Virginia retention schedules. Employees are required to file E-Mail that is required to be retained in a network folder outside of the E-Mail system.

C. Use of Citywide E-Mail Distribution

Information to be distributed by citywide E-mail should promote and support the City Council's Vision. Such messages may include information for emergency notifications, press releases, announcements, City events, etc. The City Manager, City Manager's designee or Director of Marketing and Communications must approve any distribution of information from outside organizations.

III. INTERNET USAGE

The City of Portsmouth recognizes that access to the Internet is a valuable and useful tool for employees to use in the performance of assigned duties. Internet access is intended for City business purposes. Each Department is responsible for ensuring proper and business related use.

Access to the Internet is a privilege granted upon the approval of an employee's Department Head. Department Heads are to notify the Department of Information Technology when Internet access is to be terminated.

A. 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, 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 appropriately conduct City business and does not violate City policies or any Federal, State, or local laws.

B. Internet Monitoring

Internet usage is subject to City monitoring. Internet related activity, including the identity of each user and the sites visited by each user can be recorded. Log records are subject to inspection and audit at any time for work related purposes or to determine whether violations have occurred of City policies or law.

C. Unauthorized and Inappropriate Uses

Unauthorized and inappropriate uses will result in disciplinary action, up to and including termination under the City's Employee Standards of Conduct.

The following activities are some examples of unauthorized and inappropriate uses of City computer resources, including but not limited to:

- Any use that violates the law or encourages others to break the law, and/or any use that violates the City's Employee Standards of Conduct and/or City policies.
- Use that causes harm to individuals or damage to others property, i.e. attacking someone through slander.
- Intentionally 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 or disability or any other basis prohibited by law. (The City Manager, Director of Human Resource Management or Police Chief may grant authorized employees access to such information for investigation and/or law enforcement purposes.)
- Operating a business, soliciting money, conducting business transactions for personal gain or gambling.
- Arranging for the sale or purchase of illegal drugs or alcohol.
- Intentionally disabling, impairing or overloading the performance of any computer system or network, i.e. denial of service attack, uploading viruses, Trojan horses or worms.
- Circumventing or disabling the security of any system intended to protect the integrity and security of another user or computer system, i.e. hacking.

IV. NETWORK AND INFORMATION SECURITY

Employees must respect the integrity of City network systems and electronic information. It is a violation of this policy to wrongfully access or modify files, documents, passwords or data that belongs to other users or to misrepresent oneself as someone else by accessing or using another's system or network account(s). Department Heads are authorized to request an employee's password and access to an employee's account for work related purposes.

The physical security of the City's computer resources and electronic information is the responsibility of all employees. Employees shall not permit access to the City's IT equipment to unauthorized individuals. Employees have the responsibility to protect their passwords and not share them with anyone not authorized to have them. If an employee becomes aware of a security violation or potential breach, the employee is to immediately notify their supervisor, Department Head and the Department of Information Technology.

A. Anti-Virus, Spyware and Harmful Software

The use of anti-virus software provides protection from viruses and harmful software that may damage or destroy data and City electronic resources. All City equipment will have updated virus checking software which may not be disabled or uninstalled by an employee without the permission of the Department of Information Technology.

B. Network Accounts and Passwords

Network accounts are provided for employees to access City IT resources. Each employee is required to have a unique account with a user-id and password. Employees shall take precautions to protect their network accounts and not share them with anyone not authorized to have them. Accounts should be granted only for the system privileges necessary for an employee to perform the functions for their job.

1. Establishing a Network Account:
It is the responsibility of Department Heads to authorize and define the level of system access required for an employee. Department Heads must initiate and submit Account Request Forms (available on the server at CityDocs/Forms/InformationTechnology) for new employees or position changes to the Systems Administrator (SysAdmin@portsmouthva.gov).

2. Terminating a Network Account:
Department Heads are responsible for notifying the Systems Administrator (SysAdmin@portsmouthva.gov) to inactivate or delete system accounts upon the termination or position change of an employee. The Account Request Form needs to be completed and E-Mailed to the Systems Administrator. Maintaining an active network account for a terminated employee poses potential security risks to the City's information systems and Department Heads are to promptly notify the Department of Information Technology when an account is to be inactivated. Information in an employee's terminated account will be retained for 30 days unless an extension of time is requested by the Department Head.

C. Sensitive Data

"Sensitive Data" refers to any confidential or critical information for which the loss, misuse, unauthorized access, modification or improper disclosure could adversely affect the City's interest, or the privacy to which individuals are entitled. Examples of sensitive data include but are not limited to social security numbers, driver's license numbers, medical information, health records, credit card numbers, passwords, birth dates and other personal information.

Employees have a responsibility to protect the confidentiality, privacy and integrity of sensitive data. Employees are not to share sensitive electronic information without the authorization of their Department Head.

Workstations that have access to sensitive material must be secured using network authentication and locking screen savers. Sensitive data is not to be available on public access workstations.

Sensitive data transmitted or sent outside of the City network is to be protected using encryption, Secure Sockets Layer (SSL) or other security techniques.

Employees are not to store sensitive data on laptops, mobile computing equipment or portable electronic media without following proper security procedures to protect the data. Contact the Department of Information Technology for authorized security procedures.

V. DISCLOSURE STATEMENT

I hereby acknowledge that I have been provided a copy of the Information Technology Acceptable Use Policy – August 2010 version (AP # 1) for the City of Portsmouth and that I have read it. I understand and agree to comply with the provisions of the policy stated herein. I understand that this Disclosure Statement will be placed in my personnel file as a record that I have been provided with this important policy.

I further understand that compliance with this policy is a requirement of my employment with the City of Portsmouth. Any violation of this policy may result in revocation of my information technology privileges and may subject me to disciplinary action, including termination of my employment and/or legal prosecution.

_____
Department

_____
Printed Employee's Name

_____ _____
Employee's Signature Date

_____
Printed Department Head's Name

_____ _____
Department Head Signature Date