HAMPTON COUNTY

TECHNOLOGY USAGE POLICY

Table of Contents **Page Number**

PURPOSE

1. To remain competitive, better serve the public and provide our employees with the best tools to do their jobs, Hampton County makes available to our workforce access to one or more forms of electronic media and services, including computers, e-mail, telephones, voicemail, fax machines, online services, intranet, Internet, and the World Wide Web.

2. Hampton County encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information about vendors, customers, technology, and new products and services. However, all employees and everyone connected with the county should remember that electronic media and services provided by

the county are county property and their purpose is to facilitate and support county business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

3. To ensure that all employees are responsible, the following guidelines have been established for computer use. No policy can lay down rules to cover every possible situation. Instead, it is designed to express Hampton County philosophy and set forth general principles when using electronic media and services.

TECHNOLOGY DEFINITIONS

1. Computer Virus: Software used to infect a computer and usually capable of causing great harm to the network.

2. Backup: The process of copying a file, program, or entire computer system, for use in the event that the original is in some way rendered unusable.

3. Blog: A frequent, chronological publication of personal thoughts and Web links.

4. Download: Receive a file transmitted over a network.

5. Internet and the World Wide Web: A worldwide network of computer servers connected by phone lines that allow access to the public through a special language (Hypertext Markup Language or HTML) and a special protocol (Hypertext Transfer Protocol) or (HTTP).

6. Internet Service Provider (ISP): An entity that charges startup and monthly fees to users and provides them with the initial host connection to the rest of the Internet.

7. IT: Short for ***Information Technology***. The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems within companies, universities, and other organizations.

8. E-mail: The distribution of messages, documents, files, software, or images by electronic means over a phone line or a network connection. This includes internal e-mail, external email, and Internet e-mail.

9. Encryption: A means of coding messages so they appear to be random characters. Encryption has two benefits. First, it prevents disclosure of sensitive information to unauthorized third parties. Second, encryption allows for "authentication" of the information sent.

10. Fiber Optic Cable: The science or technology of light transmission through very fine, flexible glass or plastic fibers. Used to connect

networks and to transmit telephone signals, Internet communication, and cable television signals. Due to much lower attenuation and interference, optical fiber has large advantages over existing copper wire in long-distance and high-demand applications. Fiber has higher bandwidth than copper and is the best media used today to connect networks that are in different geographical locations.

11. Social Networking: Web-based social networking occurs through a variety of websites that allow users to share content, interact and develop communities around similar interests. Examples include websites such as Facebook and MySpace.

12. Spyware: Software that sends information about your Web surfing habits to its Web site. Often built into free downloads from the Web, it transmits information in the background as you move around the Web. The license agreement that you often accept without reading may say that the information is anonymous. Anonymous profiling means that your habits are being recorded, but not you individually. It is used to create marketing profiles; for example, people that like Web sites that feature A often go to Web sites that feature B and so on.

13. UPS: Short for *Uninterruptible Power Supply.* A battery powered power supply that is guaranteed to provide power to a computer in the event of interruptions in the incoming electrical power.

14. User: as used in this policy refers to all employees, elected and appointed officials, independent contractors and other persons or entities accessing or using any of Hampton County's electronic technology resources.

15. VOIP: Short for *Voice over Internet Protocol.* A protocol for transmitting the human voice in digital form over the Internet or other networks as an audio stream, instead of using traditional telephone lines or systems. VoIP uses the Internet Protocol (IP) to provide phone-to-phone communication.

PROHIBITED COMMUNICATIONS

1. Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

    a. Discriminatory or harassing;

    b. Derogatory to any individual or group;

    c. Obscene, sexually explicit or pornographic;

d. Defamatory or threatening; or

e. In violation of any license governing the use of software.

2. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by county administration, employees are prohibited from engaging in, or attempting to engage in:

a. Any purpose that is illegal or contrary to Hampton County policy or business interests;

b. Monitoring or intercepting the files or electronic communications of other employees or third parties;

c. Hacking or obtaining access to systems or accounts they are not authorized to use;

d. Using other people's log-ins or passwords; or

e. Breaching, testing, or monitoring computer or network security measures.

PERSONAL USE

The computers, electronic media and services provided by Hampton County are for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable, but all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege. Hampton County does not accept liability for any loss or damage suffered by an employee as a result of that employee using the County Internet connection for personal use.

ACCESS TO EMPLOYEE COMMUNICATIONS

Generally, electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and instant messaging, and similar electronic media is not reviewed by the county. However, the following conditions should be noted:

1. Hampton County IT does routinely gather logs for most electronic activities or monitor employee communications directly, e.g., telephone numbers dialed,

websites accessed, call length, and time at which calls are made, for the following purposes:

a. Cost analysis;

b. Resource allocation;

c. Optimum technical management of information resources; and;

d. Detecting patterns of use that indicate employees are violating county policies or engaging in illegal activity.

2. Hampton County reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other county policies.

3. Employees should not assume electronic communications are completely private. In order for IT to effectively secure and maintain the county's network, they must have unrestricted access to all files and data.

TECHNICAL STANDARDS

IT has the responsibility for support and problem resolution for Hampton County's PCs. To effectively and efficiently carry out that role, IT must be able to rely on standard hardware and software configurations on the desktop. **Users must request hardware and software through Information Technology Department.** Users must also adhere to the naming schemes set by the IT department.

SOFTWARE STANDARDS

To prevent computer viruses from being transmitted through the county's computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Only software registered through Hampton County can be downloaded. Loading, use, and accessing of personal Internet Service Provider accounts (*i.e.* AOL, CompuServe, EarthLink, etc.) on County owned equipment is prohibited. Employees should contact the IT Director if they have any questions.

HARDWARE STANDARDS

1. All new computers purchased must have surge protection on electric power - either surge suppressor, or UPS with surge suppressor.

2. Do not install new computer hardware without the approval of the Information Technology (IT) Department.

3. Do not relocate or reassign computer equipment outside the department or between buildings without the approval of the IT Department.

4. Do not swap internal computer hardware equipment (such as network cards, video cards, hard disks, etc.) from one PC to another without authorization from a member of the IT Department.

5. Do not take computer equipment home without written authorization from the IT Department or the County Administrator (except laptops and notebooks). Employees taking ***any*** computer equipment home (including laptops or notebooks) must have permission from their department head.

6. All workstation PC's are to be shut down at the end of the day, especially during the summer, for protection against power surges from lightning storms; unless remote or network access is necessary after normal business hours.

SECURITY/APPROPRIATE USE

1. At all times when an employee is using Hampton County electronic technology resources, he or she is representing the County. Use the same good judgment in all resource use that you would use in written correspondence or in determining the “appropriate conduct”. Hampton County employees are expected to use County provided electronic resources responsibly and professionally.

2. No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

3. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

4. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

5. After employee termination, resignation, or retirement, mandatory security changes on all computer systems may be implemented. Only Hampton County employees may have access to network resources.

SOCIAL MEDIA/SOCIAL NETWORKING

The following is Hampton County's social media and social networking policy. This policy applies to all Hampton County employees that access social networking websites while on county time, and also applies to the use of all Hampton County equipment. The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guideline exists, employees should use their professional judgment and take the most prudent action possible. Consult with your manager or supervisor if you are uncertain.

1. Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the county. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the county.

2. Information published on your blog(s) should comply with the county's confidentiality and disclosure of proprietary data policies. This also applies to comments posted on other blogs, forums, and social networking sites.

3. Be respectful to the county, other employees, customers, partners, and competitors.

4. Social media activities should not interfere with work commitments. Refer to IT appropriate usage policies.

5. Your online presence reflects the county. Be aware that your actions captured via images, posts, or comments can reflect that of our county.

6. Do not reference or site county clients, partners, or customers without their express consent. In all cases, do not publish any information regarding a client during the engagement.

7. Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.

8. County logos and trademarks may not be used on social media or social networking websites without verbal or written consent.

EXAMPLES OF MISUSE

Examples of misuse include, but are not limited to, the activities in the following list.

1. Using a computer account that you are not authorized to use or obtaining a password for a computer account.

2. Using the County Network to gain unauthorized access to any computer systems.

3. Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.

4. Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.

5. Attempting to circumvent data protection schemes or uncover security loopholes.

6. Violating terms of applicable software licensing agreements or copyright laws.

7. Deliberately wasting computing resources.

8. Using electronic mail to harass others.

9. Masking the identity of an account or machine.

10. Posting materials on electronic bulletin boards that violate existing laws or the County's codes of conduct.

11. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

PASSWORDS/ENCRYPTION

1. Passwords are an important aspect of computer security. They are the front line of protection for User accounts. A poorly chosen password may result in the compromise of Hampton County's entire corporate network. Users are responsible for safeguarding their passwords for access to the computer system. Users are responsible for all transactions made using their passwords.

2. In order to provide appropriate network security, Hampton County IT must implement periodic password changes on all user accounts. Password length, password complexity, and password change occurrences may change and will be mandatory on the network.

3. Employees can use encryption software supplied to them by the IT department for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a county computer must provide their supervisor with a hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files. All wireless transmission is secured on a wireless channel. To connect to Hampton County's wireless network you must obtain an encryption key from the IT department.

WEATHER EMERGENCY

Upon activation of the Emergency Operations Center (EOC) for weather emergencies the following steps are to be taken by each User to help protect both computer hardware and software.

1. Backups should be taken of all personal computers that are not attached to the network. Both backup disk(s) and application software are to be stored in a dry and secure location for safekeeping. If the personal computer is attached to the network and the data files reside in a network directory, it is not necessary to create backups, as these files will be backed up for you. If you are attached to the network but keep data files on your hard drive, you should copy those data files (i.e. word processing documents, spreadsheets, databases, etc.) to a network directory so it may be backed up for safekeeping. Please note that every individual has a quota (a set amount of space) on the network drive. The quota is subject to change and will be set forth by the IT department.

2. All computer equipment should be powered off. This applies to personal computers; workstations, printers and any associated peripheral devices (i.e., tape backup units, modems, scanners, etc.). After powering down the equipment, disconnect the power cables from the receptacles to protect equipment from potential surges from lightning.

3. Any equipment located on the floor should be moved to a higher location and away from any windows. All monitors should be turned so that no screens face the direction of any windows.

POLICY INFRACTION

Any employee who abuses the privilege of their access to e-mail, Internet, or any other computer use in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability. All violations should be reported to the user's supervisor, manager, or the county administrator.

EMPLOYEE AGREEMENT ON USE OF HAMPTON COUNTY TECHNOLOGY

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of the county's computer and telecommunications equipment and services. I understand that I have no expectation of full privacy when I use any of the telecommunication equipment or services. I am aware that violations of this guideline on appropriate use of the county's computer systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of the e-mail and Internet may reflect on the image of Hampton County to our customers, competitors and suppliers and that I have responsibility to maintain a positive representation of the county. Furthermore, I understand that this policy can be amended at any time.

_____ _____

Print Name Department

_____ _____

Signature Date