CHESTERFIELD COUNTY
ADMINISTRATIVE POLICIES AND PROCEDURES

Department: Information Systems Technology | **Policy Number: 7-8**
Subject: Internet and Email Use | **Supersedes: 04/15/03**
11/07/01
Date Issued: 03/01/11

I. POLICY STATEMENT

The county network, which includes internet and intranet access and the electronic mail (e-mail) systems, is the property of Chesterfield County. Accordingly, the county reserves the right to review any materials transmitted across or stored in computers attached to the network. Any work related posting to the internet or intranet or Email system is a professional communication in your capacity as a county employee. The tone must be professional and the content must be accurate. Every internet posting and e-mail message must be considered the same as a signed letter written on county letterhead.

II. APPLICABILITY

This procedure applies to all full-time and part-time county employees, contractors, and volunteers connecting to the county network.

III. DEFINITIONS

A. Email Guidelines
Guidelines for email use, retention and ethics as established by a working group, the Information Technology Advisory Group (ITAG), based upon industry standards and as reviewed and approved periodically by the county Leadership Team.

B. E-mail SPAM
Unsolicited or undesired email messages, electronic junk mail, or junk newsgroup postings.

C. Encryption
Cryptographic transformation (scrambling) of information (called "plaintext") into a form (called "cipher text") that conceals the information's original meaning to prevent it from being known or used by unintended recipients.

D. Non-Disclosure Agreement (NDA)
A non-disclosure agreement (NDA), also known as a confidentiality agreement, confidential disclosure agreement (CDA), proprietary information agreement (PIA), or secrecy agreement, is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by third parties. It is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or trade secrets.

E. Uniform Resource Locator (URL)
The global address of documents and other resources on the World Wide Web. The first part of the

address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

IV. FILTERING

IST will install and maintain filtering software for all county computers. Internet filtering of county computers is in accordance with the prohibited uses described in Section VI. Exceptions to the filtering requirement may be made on an individual employee basis for appropriate governmental purposes. Department Directors should forward such requests in writing to the CIO for approval, identifying the individual employee and/or physical personal computer requesting the exception and the reason the exception is needed. IST will maintain a list of unfiltered devices and users, which shall be periodically audited by Internal Audit. The filtering of county computers does not relieve persons from the requirements specified in this procedure, nor does it provide a defense to violations of this procedure.

IST also maintains SPAM filters which automatically filters for and removes suspect or dangerous email from delivery and places them into a SPAM folder. Incoming email that could be interpreted as SPAM may include, but is not limited to, unacceptable file extensions (such as .zip files), excessively large size file attachments, objectionable content based upon subject title, and recognized malware or virus signatures. End users are provided the capability to manage their SPAM folders, but should exercise extreme caution in removing items designated by the system as SPAM.

V. SECURITY OF CHESTERFIELD COUNTY COMPUTER RESOURCES

Purpose

There are multiple threats to the security of Chesterfield County computer resources.

Email Usage

In order to prevent system overload and introduction of vulnerabilities into the environment, county employees must limit the use of the following features to work-related purposes, including but not limited to; transmission of e-mail messages to a large number of county employees, or clicking on internal or external URL links in emails. URL links in emails pose a risk of linking to a malware site that could introduce security threats to the county's network. County-wide notifications or messages shall have the approval of a department director/office administrator or a specified designee and Public Affairs. Notification methods must follow approved delivery methods based upon the need.

Accountability

Users are responsible for the use of their account and should take all reasonable precautions to prevent unauthorized persons from being able to use their account. No one shall share their passwords. For business continuity and emergencies, exceptions may be granted with CIO and Department Head approval. All passwords shall follow applicable county password management standards. It is the

responsibility of every employee to report suspected security breaches immediately to IST by contacting the IST Help Desk to report a suspected breach.

Posting or Transfer of Sensitive or Confidential Information
Sensitive or confidential information that needs to be protected for governmental business, legal or regulatory reasons must not be posted on the internet or transmitted insecurely. County employees are prohibited from sending any message or posting any information as a county employee or acting on behalf of the county, implied or intentional on the internet, personal or otherwise, that is contrary to the positions of their department or policies of the county, unless such messages are for the purpose of reporting improper or illegal actions of county employees.

VI. OWNERSHIP & MANAGEMENT OF COUNTY INFORMATION

All county owned computer systems, hardware, software, and any related systems and devices are the property of Chesterfield County. These include, but are not limited to, network equipment, e-mail, documents, spreadsheets, calendar entries, appointments, tasks and notes which reside in part or in whole on any county computer system or equipment. Accordingly, information stored on such systems or devices is also county property and subject to review at any time. There is no privacy when using county computer resources, and employees have no expectation of privacy in the use of such resources. Electronic mail records are accessible by IST staff to support system performance measurement, tuning, and troubleshooting.

Additionally, Internal Audit, HRM and the Police Department may have reason to review the electronic files of employees, which may be shared with others as necessary for legal and/or policy enforcement reasons. All county department directors shall work through the Police Department, Internal Audit or HRM to evaluate the need to review electronic records of an employee pursuant to an investigation. The Police Department, Internal Audit or HRM may then request permission from the county administrator or designee for the retrieval of the records, and forward that permission to the CIO or designee for processing. In the event an employee is unexpectedly unavailable for other than disciplinary reasons and access to the employees records is needed to support the ongoing operation of the business, the department director may request access to the electronic records from the CIO or designee.

Departments should coordinate with HRM, Internal Audit, and the Police Department pursuant to applicable county administrative procedures. Because internet e-mail passes through many computer systems en route to the recipient, it is accessible by others and is not a secure means of communication. When communicating with others, either through the county computer system on the internet, through email, or other electronic communications means, users represent Chesterfield County. The information transmitted or received can be traced and/or reported back to the county. As with any other data (whether for citizens or employees), computerized information maintained by the county is subject to federal, state and local laws. Any county business e-mail or other communications, regardless of origin,

may be subject to disclosure under the Virginia Freedom of Information Act ("VFOIA"), the Privacy Protection Act, and judicial subpoena. Since privacy cannot be assured within non-secure email systems, confidential information shall not be transmitted by e-mail.

VII. USE OF THE INTERNET AND E-MAIL SYSTEM

A. **Acceptable Use** - Employees may use county computer resources to access the Internet and transmit e-mail messages at any time for work-related purposes. Employees may use the county computer resources to access the internet and to transmit non-confidential email for appropriate non-work related purposes on personal time in accordance with the conditions governing access to their work areas as long as there is no effect on public business or job performance and such use is infrequent. This includes the use of personally owned electronic devices while at the workplace, whether connected to the county network or using a county publicly accessible Wi-Fi connection. Personal time includes breaks, lunchtime and the time before and after work. In areas where employees must share equipment or resources for network access, employees using the resources to fulfill job responsibilities always have priority over those desiring access for personal use. Use of passive, personally-owned electronic devices (i.e., personal music listening devices such as iPods, etc.) in the employee's work area is left up to the discretion of department management. Use of streaming media (such as Internet Radio) on county devices is also left up to the discretion of department management, unless it is determined by IST through performance monitoring or problem troubleshooting that its use creates a disruption or problem within the county network or on an individual work station.

B. **Prohibited Use** - The following activities are prohibited on county computer resources:

1. Intentionally accessing, viewing, downloading, uploading, posting, or transmitting information that is abusive, offensive, harassing, threatens violence, or that discriminates on the basis of race, color, religion, gender, national origin, age, or disability.

2. Intentionally accessing, viewing, downloading, uploading, posting, or transmitting sexually explicit material. Sexually explicit material includes any description of or any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting nudity, sexual excitement, or sexual conduct of any kind.

3. Operating a business, soliciting money, product advertising, or conducting transactions for profit or personal gain.

4. Using county email systems excessively for personal use. Use of county email is intended

primarily for official county business and personal use, if necessary, should be limited to incidental use and is subject to review and enforcement for abuse and misuse.

5. Gambling.

6. Arranging for the sale or purchase of illegal drugs, alcohol, or firearms.

7. Communication with elected representatives or public or political organizations via County e-mail to express opinions regarding political issues outside of work-related communications.

8. Solicitation for non-county sponsored organizations or functions.

9. Sending of countywide e-mail or e-mail broadcasts without first obtaining approval by the employee's department director/office administrator, and either the director of public affairs, or CIO, or designees. Such messages shall include a statement indicating the person that authorized the message. Don't use alternate email mailing lists (i.e., such as the HRM Liaisons Lists) to intentionally circumvent the approval process for distribution of county-wide email notifications.

10. Reproduction or transmission of any material in violation of any local, state, U.S. or international law or requirement, including material that does not comply with federal copyright laws and copying or reproducing any licensed software, except as expressly permitted by the software license.

11. Using e-mail to transmit sensitive information outside of the county network to external sources which may include information related to confidential matters, including, but not limited to; protected patient health information, criminal/juvenile records, personnel records, or records relating to legal matters, unless such information is encrypted using IST approved encryption methods and secure file transfer methods. All exchange of sensitive information with external partners requires execution of a Non-Disclosure Agreement (NDA) with the external partner.

12. Intentionally creating a computer virus and/or placing a virus on the county's network or any other network. Intentionally drafting, forwarding, or transmitting chain letters.

13. Attempts, whether successful or not, to gain access to any other system or user's personal computer data without the express consent of the other system or user.

14. Using the network, internet, intranet, or Email system in any fraudulent manner.

15. Avoiding or circumventing approved email mailbox size and capacity settings as defined by county Email Guidelines as approved by the county Leadership Team. Each employee's mailbox shall have a quota, which is a control mechanism to limit the amount and/or size of email that can be stored in or sent from the employee's county-issued email account.

16. Intentionally circumventing security and control features associated with county filtering policies or other Internet policies by using publicly accessible Internet wireless networks (such as, Citizen Wi-Fi or others) from county devices for purposes other than approved, official county government business.
17. Disregarding appropriate application of email or Internet records retention guidelines for the management of county public records as defined in *Administrative Procedure 5-6 Records Management Policy*.

18. Inappropriate usage of Social Media or Social Media web sites. Such activities include, but are not limited to:

    a. Posting proprietary, confidential, sensitive, or personally-identifiable information
    b. Speaking on behalf of the county, or giving the impression of speaking for the county, when not authorized to do so by the County Administrator or his designee(s)
    c. Speaking on county-related issues in an unofficial capacity and failing to clarify one's unofficial role of not speaking on behalf of the county
    d. Using tools or techniques to spoof, masquerade, or assume any false identity, except for approved business or law enforcement purposes as approved through county policy or by legal statute

19. Downloading or installing software without IST approval.

20. Auto-forwarding of county email which constitutes official county government correspondence to a personal email account (such as Yahoo, GMAIL, or other internet based email accounts), which reduces the ability to routinely manage the content in accordance with Administrative Procedures; 7-6 Release of Information and county records retentions guidelines as defined in 5-6 Records Management Policy.

21. Forwarding of inappropriate email (such as politically sensitive or otherwise offensive jokes, chain letters, or other harassing or spam-like communications) of a personal nature representing a county correspondence to external Internet email addresses which has the potential to adversely affect the county's image, reputation, or Internet-based email ethics reputation.

22. Any other use of the network that violates Chesterfield County policies or Code of Ethics.

VIII. USE OF INTERNET BASED SYSTEMS AND SERVICES

Approval for Use of Internet-Based and/or Internet Hosted Business Solution Systems and Services

Internet-based or hosted systems may be available generally to the public without cost, at a minimal cost, or for more robust versions of the system/service for a significant cost. Regardless whether the system or service is free or requires some costs, authorization to accept Terms of Service (TOS) for Internet-based or Hosted Business Solution Systems or services must first receive approval from Chesterfield County's Chief Information Officer (CIO), Purchasing Director and County Attorney, or their designees. No county employee is authorized to accept or agree to an Internet-Based TOS without first obtaining this approval.

Internet-based Systems Vendor Management Roles and Responsibilities

Information Systems Technology (IST) has primary responsibility for managing the vendor technology relationship for all Internet-based or hosted Business Solution systems and services for the purpose of assuring appropriate technology practices are applied related to technology architecture, information system security, service level agreements, operational processes, technical support and business continuity.

Information Security Management of Internet-Based and/or Internet Hosted Systems and Services

The county Information Security Manager has ultimate responsibility and approval authority to examine system risks and require appropriate assurance levels of information security controls for all systems, including Internet-Based and/or Internet Hosted Systems and Services, pursuant to the county *Administrative Procedure 7-3 Information Security Policy.*

IX. DISCIPLINARY ACTION FOR VIOLATION OF THIS ADMINISTRATIVE PROCEDURE

A. Any employee who intentionally receives, accesses, views, transmits, or downloads sexually explicit material from the internet on county computer equipment will be disciplined up to and including termination. Sexually explicit material is defined as any description of or any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting nudity, sexual excitement, or sexual conduct in any form. Persons subscribing to an email list will be viewed as having solicited any material delivered by the list, as long as that material is consistent with the purpose of the list. Likewise, persons conducting a search on the internet will be viewed as seeking any results generated by the search, as long as that material is consistent with the search.

B. Any employee who commits or is convicted of a crime related to the use of county computer equipment shall be terminated.

C. Any employee who violates any provision of this policy, unless required to do so as part of his or her assigned and authorized job responsibilities, shall be disciplined in the following fashion:

1. Any employee whose use of Chesterfield County's computer resources results in damage to those resources will be required to reimburse the county for the cost of repair and reconfiguration, as well as the hours required for the repair work, and costs associated with replacing necessary hardware or software. Where damage occurs as the result of inadvertent actions, without the intent to cause damage, the employee causing the damage will not be asked to reimburse for such damage.

2. In determining the appropriate disciplinary action to be taken against an employee under this policy, supervisors shall apply the standards set forth in the Personnel Policies of the county for appropriate situational discipline (Section 4-2) and shall ensure that the employee Code of Ethics (Section 1-4) is maintained. In addition, supervisors shall consider the nature of the employee's job responsibilities, and the legality or illegality of the violation in determining the appropriate disciplinary action. Discipline may include any of the options contained in Section 4-3 of the Personnel Policies, including, but not limited to:

   a. Suspension of access to e-mail or internet services.
   b. Restitution or reimbursement for the hours used to conduct personal business on county computer resources in violation of this policy.
   c. Other disciplinary action(s) as outlined in Chapter 4 of Chesterfield County Personnel Policies.
   d. Termination of employment.