Email/Internet Use

Welcome to the:

Internet and Email Use Policy 7-8

Job Aid

Enter

Welcome! Thank you for accessing this job aid! It is intended to help you understand and apply appropriate use of the **7-8 Internet & Email Use Policy**. You may use the arrow buttons in the navigation menu to review each page of the job aid or you may use the table of contents to review a specific topic. If you require help using this job aid, please contact Sherri Dosher within the Center for Organizational Excellence at 717-6614.

On each page is a navigation menu in the bottom right corner:

- The **Right** and **Left** arrow buttons will take you forward and back one page.
- The **Home** button will take you back to this summary page.
- The **Question** button will allow you to send a question or feedback by email.
- The **Document** button will take you to the IST website where you may download a printable version of the policy at any time.
- The **End** button will take you to the final page for additional resources and the exit button.

Table of Contents

Policy Statement

connected Government
STAYING CONNECTED WITH CHESTERFIELD

The county network, which includes internet and intranet access and the electronic mail (e-mail) systems, is the **property of Chesterfield County.**

- 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**.

Applicability

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Who is the policy for?

- Applies to all full-time and part-time county **employees, contractors, and volunteers** connecting to the county network.

Does that mean me?

- **If You Connect**, then the policy applies to you!

Definitions

connected Government
STAYING CONNECTED WITH CHESTERFIELD

- **Email Guidelines**

  Guidelines for email use, retention and ethics based upon industry standards.
- **E-mail SPAM**

  Unsolicited or undesired email messages, electronic junk mail, or junk newsgroup postings.
- **Encryption**

  Scrambling of information into a form that conceals the information's original meaning to prevent it from being known or used by unintended recipients.
- **Non-Disclosure Agreement (NDA)**

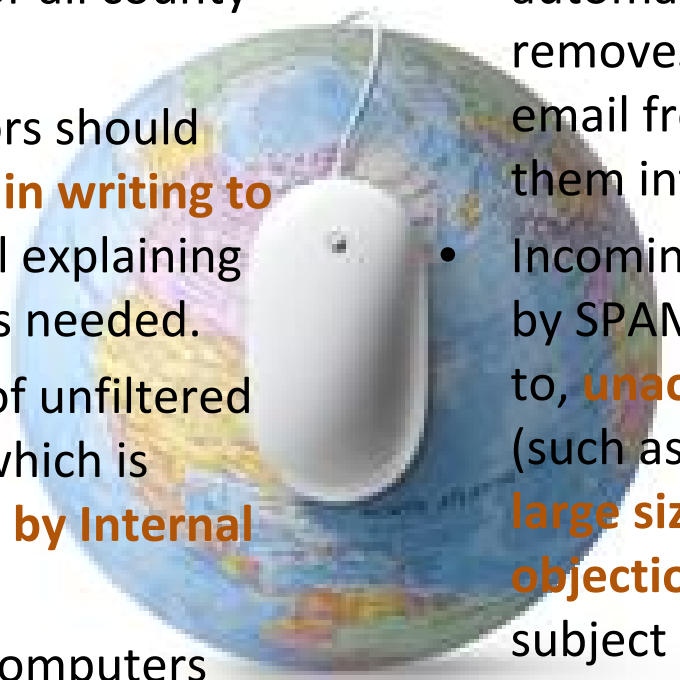
  A contract through which the parties agree not to disclose information covered by the agreement.
- **Uniform Resource Locator (URL)**

  The global address of documents and other resources on the World Wide Web.

Filtering

connected Government
STAYING CONNECTED WITH CHESTERFIELD

- IST will install and maintain **filtering software** for all county computers.
- Department Directors should forward **Exceptions in writing to the CIO** for approval explaining why the exception is needed.
- IST maintains a list of unfiltered devices and users, which is periodically **audited by Internal Audit.**
- Filtering of county computers **does not relieve employees** from following this policy.



- IST 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 may be caught by SPAM 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.

Security

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Email Usage – **Don't Do this!**

- **E-mail messages to a large number of county employees** – follow approval process below.
- **Click on external URL links** in emails. URL links in emails pose a risk of linking to a Virus/Malware sites that could introduce security threats to the county's network.
- **Send County-wide notifications or messages** without approval of a department director/office administrator or a specified designee and Public Affairs.

Security

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Accountability – Be responsible for your Activity!

- **Don't let others use your account!**
  - 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.
- **Don't Share your Password!**
  - **No one shall share their passwords.** For business continuity and emergencies, exceptions may be granted with CIO and Department Head approval.
- **Make it a Good, Strong Password!**
  - 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.

Security

connected Government
STAYING CONNECTED WITH CHESTERFIELD

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.

Ownership & Access

connectedGovernment
STAYING CONNECTED WITH CHESTERFIELD

Who Owns the Data? Chesterfield County Does!

- **It's county property and subject to review at any time!**

  All county owned computer systems, hardware, software, and any related systems and devices are the property of Chesterfield County. Such as; network equipment, e-mail, documents, spreadsheets, calendar entries, appointments, tasks and notes & data stored on the systems or devices .

- **No expectation of privacy**

  There is no privacy when using county computer resources

- **All access & data is Monitored**

  Electronic mail records are accessible by IST staff to support system performance measurement, tuning, and troubleshooting.

Ownership & Access

connectedGovernment
STAYING CONNECTED WITH CHESTERFIELD

Who Can See My Data? IST, HRM, Police, Internal Audit, and others!

- **Maintenance & Monitoring Access**
  - IST is responsible for the health and well-being of all county systems and data and **conducts normal monitoring activities for all county data**. In the course of that work is authorized to access all county information.
- **Investigative Access**
  - 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.
- **Business Continuity Access**
  - 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.

Ownership & Access

connectedGovernment
STAYING CONNECTED WITH CHESTERFIELD

Who Can See My Data? IST, HRM, Police, Internal Audit, and others!

- **Subpoenas, FOIA, Oh My!**

  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**.

  You may as well mail a Postcard!

  Since privacy cannot be assured within non-secure email systems, **confidential information shall not be transmitted by e-mail**.

Use of Internet & Email

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Acceptable Use

- **Job- Related**
  - May access the Internet and transmit e-mail messages at any time for work-related purposes
- **Personal Time (Infrequent Use)**
  - May access the internet and to transmit non-confidential email for appropriate non-work related purposes on personal time. Personal time includes breaks, lunchtime and the time before and after work.
- **Personal Devices**
  - May use personally owned electronic devices while at the workplace, whether connected to the county network or using a county publicly accessible Wi-Fi connection

- **Workspace Appropriateness**
  - 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. 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.
- **Department Discretion**
  - Use of passive, personally-owned electronic devices (i.e., **personal music listening devices such as iPods**, etc.) and use of streaming media (such as **Internet Radio**) in the employee's work area is left up to the discretion of department management.
- **Performance Priority**
  - May use limited network resources only. If IST determines that personal use is creating a disruption or problem within the county network or on an individual work station IST may prioritize network resources as necessary.

Use of Internet & Email

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Prohibited Use

1) 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) Accessing, viewing, downloading, uploading, posting, or transmitting **sexually explicit material**.
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.**
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
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.

Use of Internet & Email

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Prohibited Use

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 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
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*.

Use of Internet & Email

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Prohibited Use

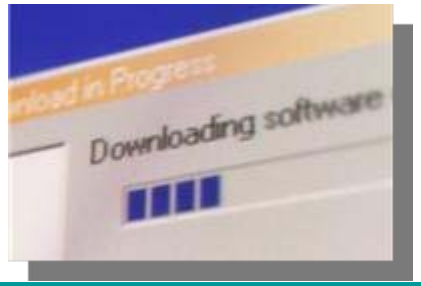
18) **Inappropriate usage of Social Media** or Social Media web sites.
   - **Posting proprietary, confidential, sensitive, or personally-identifiable information**
   - **Speaking on behalf of the county**, or giving the impression of speaking for the county, when not authorized to do so by the County Administrator or his designee(s)
   - **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
   - 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)

21) **Forwarding of inappropriate email** (such as politically sensitive or otherwise offensive jokes, chain letters, or other harassing or spam-like communications)

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



Use of Internet Systems

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Use of Internet Based Solutions

- **Approval to Use Internet Systems**
  - **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.
- **Roles & Responsibilities**
  - **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**
  - 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.*

Disciplinary Actions

connected Government
STAYING CONNECTED WITH CHESTERFIELD

Disciplinary Actions

- **Sexually Explicit Material**
  - 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. 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.
- **Criminal Activity**
  - Any employee who commits or is convicted of a crime related to the use of county computer equipment shall be terminated.
- **Violation of Policy Provisions**
  - 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. Discipline may include any of the options contained in Section 4-3 of the Personnel Policies, including, but not limited to:
    - Suspension of access to e-mail or internet services.
    - Restitution or reimbursement for the hours used to conduct personal business on county computer resources in violation of this policy.
    - Other disciplinary action(s) as outlined in Chapter 4 of Chesterfield County Personnel Policies.
    - Termination of employment.

Resource Page

Additional Questions?

- IST Policies & Procedures Page
- istsecurityservices@chesterfield.gov

Thank you for using this job aid!

To end, Click the Exit button below.