

**CHARLES COUNTY GOVERNMENT
Policy/Procedure**

SOP# CC.1.005



| Approved: August 2, 2001

| Revised: April 27, 2010

| Revised: January 25, 2011

Approved by: *Constance Kelly*

PROCEDURE: Information Technology Use and Security Policy

1.0 PURPOSE

1.1 The purpose of the *Information Technology Use and Security Policy* is to help protect Charles County Government, its employees, and any authorized user of Charles County's Information Technology from liabilities and service interruptions due to inappropriate use of Charles County's desktop/laptop computers/terminals and/or information technology services and breaches of information technology security.

1.2 Information technology means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information. Information technology systems/tools are to be defined as all hardware, software, and any automation services or tools owned or licensed to Charles County Government and available for "official use" by Charles County employees and all authorized personnel including, but not limited to, desktop/laptop computers/terminals and related peripheral equipment and software, voice mail, Internet connectivity and access to Internet services, and E-mail.

2.0 POLICY

2.1 This policy documents the authorized user's responsibility to safeguard the desktop/laptop computer/terminal equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It provides guidance for the use of Charles County Government's Information Technology through a responsible, efficient, ethical and legal manner for "county business purposes" only, in accordance with the mission, policies and operating procedures of the Charles County Commissioners. Users may be disciplined for noncompliance with this policy. This policy does not purport to address every information technology operating and security issue. It is the user's responsibility to use sound judgment. Should a user identify an issue or situation that they are not certain how to deal with, they should inquire of management. The *Information Technology Use and Security*

Policy is subordinate to any employment contract or other employment agreements. Charles County Government may add to, or change, the policies at any time. Annual Awareness Training will be conducted and must be attended by all users of Charles County's Information Technology. Please read the policy carefully and sign the "Information Technology Use/Access Release" form attached. The signed form should be given to your supervisor, signed by the Department Head, and then forwarded to Information Technology.

3.0 REGULATION AND USAGE

3.1 General Guidelines

a. Use for Authorized Purposes Only

The use of all Charles County Information Technology systems/tools is restricted to authorized purposes only. Under no circumstances shall Charles County Information Technology systems/tools be used for any commercial purpose, or to publish, disseminate or communicate any material of a political, religious, obscene or derogatory nature.

Charles County Information Technology systems/tools may not be used for the following:

- Violation of any public laws;
- Using profane or obscene language or graphics;
- Copying commercial software in violation of copyright law;
- Using the network resources for personal financial gain or any commercial or illegal activity; or
- Permitting any users/persons access to tools, network systems and applications who have not been authorized or established as a valid user by Charles County Government and Information Technology (IT).

Use of Charles County Information Technology systems/tools for any of the above may be grounds for dismissal, disciplinary measures for future use of equipment and any or all of the above or other personnel measures as may be described in the Charles County Personnel Policy and Procedure Manual.

b. Personal Use

Charles County employees are permitted use of Charles County Information Technology systems/tools for personal needs if the use does not interfere with official business and involves *no additional expense* to Charles County. *No additional expense* means that employee's personal use of county equipment is limited to those situations where the county is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the county. This *personal use* of Charles County's Information Technology systems/tools should take place during the *employee's non-work time*.

This *privilege* to use Charles County's Information Technology systems/tools for non-county business may be revoked or limited at any time by this policy or departmental management. *Privilege* means, in the context of this policy, that Charles County Government is extending the opportunity to its employees to use county equipment for personal use in an effort to create a more supportive work environment. However, this policy does not create a right to use county equipment for non-county business. Nor does the privilege extend to modifying such equipment, including loading personal software or making hardware configuration changes.

c. Inappropriate Uses

Charles County employees are expected to conduct themselves professionally in the workplace and refrain from using county equipment for activities that are inappropriate. Misuse or inappropriate use of county equipment includes but not limited to:

- Any use that could cause congestion, delay, or disruption of services to any Charles County Information Technology systems/tools. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use.
- Using the Charles County Information Technology systems/tools as a staging ground or platform to gain unauthorized access to other systems.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority.
- Any use that could generate additional expense to the Charles County Government.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

d. Protect Your Computer Equipment

All authorized users share in the responsibility to protect Charles County's desktop/laptop computer/terminal resources from physical and environmental damage/loss. Users are responsible for the correct operation and physical security of Charles County's Desktop/Laptop computers or terminals. Destruction, theft, alteration, or any other form of sabotage of Charles County's Information Technology systems/tools is prohibited and will be investigated and prosecuted to the fullest extent of the law.

e. Use Only Approved Software

Software installed on and/or used by Charles County's desktop/laptop computers must be approved and installed by IT. IT will maintain all Charles County approved software media, its licenses and documentation. Only IT approved and installed programs and systems may be used by Charles County employees or authorized users on Charles County equipment.

Charles County Government does own some software applications. These applications were developed in-house. Charles County Government does not own all of the software used, but rather licenses the right to use software. Accordingly, county licensed software may only be reproduced by IT personnel in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. This includes photocopying of the user and operational manuals. Copyright laws apply on the Internet as well. Copyright infringement is serious business, and Charles County strictly prohibits any such activity.

f. Computer Hardware Configuration Changes

Only IT can authorize configuration changes to any computer hardware submitted via a Work Request. Only IT personnel can install or replace computer hardware including but not limited to zip drives, sound cards, etc.

g. Protect Your Password

Do not share your password with anyone. Do not write it down where someone can find it. Do not send it over the Internet, E-mail, or dial-up modem without an acceptable encryption technology. Users will be held accountable for activity performed under their password. Select difficult passwords. Change them regularly, and protect them.

h. Protect Your Computer When Logged on

Desktop/Laptop computers or terminals shall not be left unattended whereby inappropriate access to Charles County Government owned/held information may be gained by unauthorized persons. Employees should log-off when leaving their work-area for 30 minutes or more.

i. Guard Against Computer Viruses

The end user shall virus scan all files which are downloaded from the Internet or brought in on magnetic media from outside sources for work related purposes. IT provides current anti-virus scanning software to allow users to perform this task. It is the end user's responsibility to make sure that they understand how to use the anti-virus scanning software.

j. Maintain Password Encryption

Various programs allow users to password protect individual files. All individual password protected documents shall have the password removed upon request by Department Director, an Information Technology employee or prior to separation of employment with Charles County Government.

k. Prevent Data Loss

Users are responsible for the protection of essential data files and the security of important, confidential, or private information. Storing of these files and information on the desktop computer disk drive cannot ensure protection or security of the information. All important, essential, confidential, or private information must be stored on Charles County Government Network (CCGNET). Storing information on the Desktop computer is prohibited without prior authorization. CCGNET is equipped with electronic and physical security. Activity on CCGNET is monitored for tampering, and other security breaches. Maintenance and back up are performed on CCGNET daily. Programs and other information are updated on the CCGNET as necessary. Use CCGNET; it is safe, effective, and reliable. It is the end user's responsibility to make sure that they understand how to use CCGNET.

3.2 Electronic mail

a. Only Essential E-mail Should Be Saved

Employees should only retain e-mail that is of importance in a folder within GroupWise. Non-essential e-mail should be disposed of once it's acted upon. Refer to the Email Retention policy for retention and archiving procedures.

b. Charles County Government's E-mail Is Public Record

There is no "right to privacy" in e-mail communications. E-mail messages (both internal and via the Internet) constitute a public record and may be subject to public disclosure in accordance with applicable law.

c. CCG E-mail Best Practices

1. Unique IDs: The naming convention for e-mail user IDs ensures that each user ID is unique system-wide. This ensures unique Internet addresses, and those addresses will continue to work correctly even after users are moved between GroupWise post offices.

2. Archiving: Archiving is a means to move messages (mail, tasks, appointments, notes, and phone messages) to a specified directory on a network server, reducing the burden of messages which the e-mail system must manage. The e-mail system will automatically delete mail items older than 180 days. See E-mail Retention policy for more information.

3. Attachments: E-mail should not be used for the wide distribution of large attachments. Sending graphics (.jpg, .bmp, etc.) large sound files (mdi, wav), and movie files (avi) to multiple users is strongly discouraged. Shared/Common directories exist for the purpose of sharing of large attachments.

4. Capitalizing: Capitalizing whole words is generally considered shouting. Asterisks surrounding a word can be used to make a stronger point.

5. Subject Title: Make it easy for the reader to quickly locate messages by including an appropriate subject title for the message. Messages should be concise and to the point.

6. Chain Letters, Spam, and Hoaxes: Do not pass around e-mail chain letters. Do not Spam. Spam is unsolicited commercial e-mail (including non-approved fund-raisers). Don't pass around e-mail hoaxes. If a hoax is received, forward to IT only, so that IT can validate the hoax and then take appropriate action.

7. Training: CCG provides basic e-mail training for end-users. CCG's e-mail software (GroupWise) is a powerful collaborative tool. Users are trained on calendaring, CCG's resource sharing/scheduling, and the function of proxies.

d. Use E-mail as Appropriate

E-mail can be a powerful, productive and time-saving tool when properly used. It is not however, a substitute for other necessary and appropriate forms of communication. When improperly used, e-mail can unnecessarily absorb valuable time and personal resources by requiring the daily review of large numbers of messages which may be unnecessary or more appropriately conveyed through face-to-face communication. For example, generally e-mail should not be used to communicate *sensitive* personnel information either to or about an employee. Counseling and/or reprimanding an employee via e-mail rather than a direct meeting is not appropriate. Additionally, in some instances more individuals than necessary may be copied on e-mail messages in an effort by the sender to cover all bases or shift some burden to message recipients. E-mail does not absolve the sender of necessary and appropriate verbal or in-person follow-up responsibility.

e. Sending Group E-Mail

1. Departments should be extremely judicious in sending unsolicited email to all employees using "ALL CCG" group that direct mails to everyone on the GroupWise mail system.
2. When improperly used, e-mail can unnecessarily absorb valuable time and personal resources.
3. E-mail should not be used to communicate sensitive personal or personnel information.
4. Department Heads should review large group messages originating from their departments for appropriateness before the message is sent.
5. The GroupWise email system is County property and thus falls under the Information Technology Use and Security Policy for use in official County business.

6. Messages sent to the "ALL CCG" group consume enormous amounts of employees' time to read and storage space on the IT systems, especially with image and file attachments. Messages with attachments for "ALL CCG" should be established by contacting the Webmaster. The recipients of the e-mail will only need to click a link to open the image and/or file attachment.

7. Anyone sending a message to large groups of GroupWise recipients must include his/her e-mail address, telephone number and departmental affiliation in the message so that recipients can easily identify the sender.

8. When sending a large email, place all but one of the addresses in the blind carbon copy ("Bcc:") field of the message. If the addresses are on the "Bcc:" field rather than the "To:" or "Cc:" fields, a reply to the message will go only to the original sender, not to the entire list of addressees therefore reducing the number of replies which could create another mass mailing.

9. Departments that make frequent or regular large group mailings are encouraged to maintain their own groups. Messages to these groups should have an introduction indicating willingness to remove an individual from the group if requested by return e-mail.

10. Keep mailing groups/lists current.

f. **REPLYING TO GROUP EMAIL:**

1. When replying to group email, just reply to the author to avoid spamming the others in the group.

2. When replies do go to all of the original addressees, each reply is also considered a mass mailing.

3. It's best to type in the address instead of relying on "reply."

4. The auto-reply feature in GroupWise is useful for in-house, however, users are discouraged from sending to entire mailing lists. The auto-reply feature should be set to "reply to sender."

3.3 Internet

a. **Internet Use/Access**

Internet use/access will be only used for official Charles County Government business except as provided for in 3.1b. Employees and authorized users will not operate a business through the Charles County Government's Internet link.

b. Guard Against Viruses

Take all required precautions against importation of computer viruses. This includes virus scanning files obtained through the Internet utilizing the virus scan software provided by the Information Technology (IT) *before* the file is accessed in any way.

c. List Server Subscriptions

Employees and authorized users will not subscribe to any non-work related list servers, nor access any chargeable site without prior County Administrator authorization.

d. Inappropriate Site Access

Employees and authorized users will not access violent, pornographic or other inappropriate sites through the Internet.

e. Streaming Video or Audio Sites

Employees and authorized users are not permitted to access or download streaming video or audio.

3.4 Violations

Misuse of Charles County's desktop/laptop computers/terminals and/or information technology services and breaches of information technology security is a violation of this policy and procedure and may result in disciplinary action, up to and including termination of employment.

4.0 USE OF SOCIAL MEDIA

4.1 Definitions:

a. Social media are media for social interaction, using web-based technologies to turn communication into interactive dialogues. Social media are works of user-created video, audio, text or multimedia that are published and shared in a social environment, such as a blog, wiki or video hosting site using software tools such as Facebook, MySpace, Flickr, etc. Youtube, commonly referred to as social media, is NOT blocked and is accessible on the County network for use by employees in accordance with this policy for training, etc.

4.2 Guidelines:

a. The County use of social media will be implemented and evaluated in phases. Initial use of social media will be limited to Facebook using one way conversation i.e.: "likes", no "friends". Only one County account with one User ID and Password will be permitted on Facebook.

b. Access to social media will not be available on the County Government network (with the exception of YouTube). Access will be limited to authorized staff in each department using a computer that has access through a data card or other means approved by the IT Division. The Department Head will authorize certain staff to access social media for official County use in accordance with this policy.

c. Use of any social media on work time must be performed in adherence with the employee's direct scope of work and responsibilities.

d. Employees should write in third person and identify themselves by Department and/or Division, as applicable.

e. When placing materials and information on social media, put a link to the CharlesCounty.org URL that is relevant to the posted information.

f. Staff authorized to use social media are responsible for complying with applicable federal, state and county laws, regulations and policies. This includes adherence to established laws and policies regarding copyright, records retention, Freedom of Information Act (FOIA) and other protected information such as Personal Identifiable Information (PII). Confidential information such as HIPAA protected content must remain confidential.

g. These guidelines may continually evolve as new technologies and social networking tools emerge. The Chief Information Officer will review social media site usage and provide policy recommendations to the County Administrator on a continuing basis.

h. County-wide access will be available on the network to such programs as Flickr, Picasa and Shutterfly for promotional use.

5.0 POLICY ADMINISTRATION AND REVIEW

5.1 Privacy Rights

Information Technology (IT) and designated system administrators may, from time to time, have need to review both employee messages and/or Internet use/access. E-mail on CCGNET servers is the property of Charles County Government. This policy allows for the e-mail administrator access to mailboxes for any of the following purposes:

- To retrieve lost messages; or
- To recover from system failures or monitor system performance.

This policy also requires approval from the Assistant County Administrator and/or County Administrator before the e-mail administrator can access mailboxes for personnel issues or suspicion and any of the following:

- To comply with investigations into suspected criminal acts;
- To ensure that CCG's systems are being used for CCG business purposes only;
or
- For any other purpose authorized by the County Attorney.

5.2 Monitoring Usage

All supervisors within the CCG's departments are responsible for ensuring that their employees are aware of these policies and procedures and adhere to them. Department Heads will require a signed "Information Technology Use/Access Release" form from authorized users, signed by the Department Head and then forwarded to the Information Technology (IT) prior to access activation. Signed access authorization forms will be included in employee's personnel record (within IT).

5.3 Departments Are Responsible To Notify IT

The departments are responsible for providing notification to Information Technology (IT) via the Work Request System when an authorized user (Full-Time or Part-Time) begins changes or ends employment with Charles County Government. Non-employee authorized users no longer needing access requires IT being notified immediately and documented via a Work Request.

6.0 Exceptions

- 6.1** Provisions of this policy may be waived at the discretion of the County Administrator. Any and all exceptions to this policy must be approved in advance.

INFORMATION TECHNOLOGY USE/ACCESS RELEASE

A signature is required on this release form before a Charles County Government Employee or any authorized user is permitted use/access of Charles County's Information Technology. By signing this release, the employee or authorized user agrees that he/she has read and understands the *Information Technology Use and Security Policy*, will abide by this policy and will take annual security awareness training, when made available by Charles County Government.

This employee or authorized user acknowledges that all Information Technology systems/tools, its messages and materials transmitted by, received from, or stored therein are the sole property of the Charles County Government. In addition, the Information Technology shall be used strictly for legitimate business purposes to promote the Charles County Government's interests and shall not be used for either personal use or to store, transmit or download prohibited material.

Employee or Authorized User Name (please print)

Network User ID

Employee or Authorized User Signature

Date

Department Name

Department Head Approval

For IT Use Only

Received: _____ User ID: _____ Server ID: _____