Greenville Technical College
Administrative Policies

5-12 Computer Use and Electronic Media

Insertion Date: 8-11-10
Revision Date:
Removal Date:

Approved by President:
Keith Miller

Automated information and information resources owned or managed by Greenville Technical College provide access to information technology and resources for students, faculty members, staff members, and other authorized users within institutional priorities and financial capabilities. The Information Technology Responsible Use Policy ensures responsible use of the College's information technology resources, protecting automated information and information resources against accidental or unauthorized disclosure, modification or destruction, as well as assuring the security, reliability, integrity, and availability of information at the College. Greenville Technical College reserves the right to extend, limit, restrict, or deny computing privileges and access to its information resources as well as to monitor the utilization of information resources by authorized users.

Users are reminded that all information created or received for work purposes and/or contained in College computing equipment files, servers or e-mail are depositories and are public records, and are available to the public unless an exception to the South Carolina Public Information Act applies. Thus, users should have no expectation of privacy. The College respects the desire for privacy and voluntarily chooses to refrain from routinely inspecting user files and electronic/telephonic communications. However, the College may monitor access to the equipment and networking structures and systems for such purposes as insuring the security and operating performance of its systems and networks; and enforcing College policies, procedures, guidelines, and applicable laws.

Users shall adhere to a standard of behavior that is not disruptive to the business of the College and will not create what even a casual observer might reasonably perceive to be an atmosphere of harassment. Users will be good stewards in the care and safeguarding of files and records and will be certain to not leave themselves logged into any unattended system.

All users, by accessing any College information resources are certifying that they understand and accept the provisions of this Policy and may be subject to disciplinary action up to and including termination for infringements of this policy. "Users" may be defined as students, employees or community members.

Complete Information Technology Responsible Use Policy – Appendix

Examination of users' files, email, or network transmission contents by the Office of Information Technology staff or its contractors must be authorized beforehand. **Click here for policy process**.

The use of a college-provided password or code does not restrict the college’s right to monitor the e-mail system, Internet access, or the files, drives, or disks on any college assigned computer or terminal. Therefore, employees have no right of privacy in any e-mail or Internet communications or information that they transmit, receive or delete, and no privacy right exists in any files and data that employees store on the college’s computer system or on their assigned computers or disks.

Employees are not authorized to retrieve or read any e-mail that is not addressed or sent to them. The college’s confidential business information and student records shall be preserved and shall not be disclosed or disseminated to employees or others outside the college who are not authorized to receive the information. No materials shall be downloaded from the Internet without the prior approval of the employee’s supervisor.

The college’s e-mail system and Internet access shall not be used to harass employees or other persons through transmission of, for example:

1. Profanity

2. Sexually oriented language, sexually explicit materials or jokes, or other offensive or derogatory information of a sexual nature, or

3. Comments of a racial, religious or other discriminatory nature.

Any employee who violates the college’s computer, e-mail and Internet use policy shall be subject to discipline, up to and including discharge.

Computer Security and Responsible Use:
Frequently Asked Questions

General

Q: Why do we need a Computer Security and Responsible Use Policy?

A: The College is increasingly relying on technology and information resources. The Computer Security and Responsible Use Policy assists users in understanding how College values, such as, integrity and creating a learning organization, are supported through our information resources.

Q: Are there "special rules" in place because computers are involved?

A: Not really. Wherever possible the *Computer Security and Responsible Use Policy* points to existing policies, and other existing College documents and clarifies that these documents also apply to activity on the College computer systems. There are two key points to keep in mind. First, each user is responsible for the intended and unintended consequences of their actions. Second, in a given situation, it's important to ask the question: "What would be the response if this happened and it didn't involve a computer?" In most cases, this answer would be the appropriate response.

Passwords

Q: Can I share my user password with others? Or can I log in and then let someone else use my account?

A: No. Someone else using your user name and password assumes your identity on the system. Most people would never consider letting others use their driver's license or other "real life" identification. Passwords should be taken just as seriously.

Q: What do I do if my supervisor asks for my password?

A: It would be against College policy for your supervisor to request or for you to give out your password. There are technology tools such as shared drives which allow users to share files or provide access to important information.

Privacy & Security

Q: How secure is my e-mail?

A: It is a good general rule to assume that any information in an e-mail sent over the Internet is available to the general public unless the message is encrypted. It is strongly recommended that the College e-mail system **not** be used to send confidential or sensitive information.

Q: How 'private' is my activity on the network?

A: There's a tremendous amount of information which is logged behind the scenes when you are on the network. This information is needed for troubleshooting problems and to insure network stability. For example, our mail system routinely logs the source and destination of all incoming and outgoing Internet mail. These logs are archived and are available for technical staff if needed. Troubleshooting network performance problems sometimes requires tools which enable technicians (both within the College and all along the Internet path) to see which workstations are visiting which Internet sites. Some Internet sites log information about you behind the scenes every time you visit their site. Your workstation itself may provide a rich history of your networking activity.

Q: What if I have sensitive, confidential, or private files that I do not want others to access?

A: Any file on a College system has the potential of being accessed by an authorized College employee or agent if sufficient cause for the access has been established. (This is a very rare event.) Storing confidential information on removable media such as a USB key may be secure as long as you don't misplace the media. Other options (in descending order of the protection they provide) are a local workstation hard drive (C:) if the computer is in a secure area; a personal network drive (usually H:), or a shared drive (usually T:). Confidential information should never be stored on 'public' drives.

Q: If my password gives me access to sensitive or confidential information, is it OK to look around just to see what I can see.

A: No. Users with access to confidential or sensitive information have a special trust. They must use their special access only for College purposes. For example, it is **not** appropriate for a user with access to confidential student information to look up records of children or friends. Similarly, it is **not** appropriate for technical services staff with special access privileges to look at files on the system out of curiosity. In both cases, users have violated the policy and would be subject to the consequences.

General Responsibilities

Q: What is the supervisor's role in enforcing the *Computer Security and Responsible Use Policy*?

A: The supervisor's role is no different for this policy than any other College policy. Supervisors are responsible for ensuring that their employees are aware of the policy and what it means, for taking reasonable precautions to ensure a secure environment for information resources, and for following up on any suspected violations.

Q: What needs to be reported and to whom?

A: If you suspect that the *Computer Security and Responsible Use Policy* has been violated, contact either your supervisor or Human Resources.

Greenville Technical College

Information Technology Services
Computer Security and Responsible Use Policy
Appendix

1. General Statement. Automated information and information resources owned or managed by Greenville Technical College provide access to information technology and resources for students, faculty members, staff members, and other authorized users within institutional priorities and financial capabilities. Although Greenville Technical College takes measures to safeguard integrity and confidentiality, it in no way guarantees the safety or security of information resources. Greenville Technical College disclaims liability for the unauthorized interception, use, misuse, damage or destruction of information resources. No student, faculty member, staff member, or authorized user shall seek to hold Greenville Technical College liable for damage resulting from unauthorized interception, use, misuse, damage or destruction of information resources. Each authorized user shall hold Greenville Technical College harmless and indemnify it for any expense or loss caused by his/her own unauthorized interception, use, misuse, damage, or destruction of information resources, or by his/her violation of this Policy.

   It is the policy of Greenville Technical College to take all reasonable measures to protect its information resources and to ensure these resources are used for their intended purposes. The administration of the College will develop and implement guidelines and procedures to ensure responsible use of its information technology resources and to protect automated information and information resources against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity, and availability of information at the College. Such guidelines and procedures are not intended to infringe upon the academic freedom rights and responsibilities of faculty members.

   Greenville Technical College reserves the right to extend, limit, restrict, or deny computing privileges and access to its information resources as well as to monitor the utilization of information resources by authorized users.

2. Definitions. The following definitions apply to this policy:

   (a) "Information Resources" include, but are not limited to, all College owned or managed:

   - information processing and telecommunications hardware, software, and computer media;
   - security access codes including passwords and;

- information that is transmitted, stored, printed, and/or processed by a computer system.

(b) An "Authenticated User Account" is an account established on an information resource which includes a user name and password and is designed to uniquely identify a specific individual to the information system for the purpose of providing resources to that user.

(c) "Confidential Information" maintained by the College is exempt from disclosure under provisions of the Freedom of Information Act or other applicable state or federal laws. Programs and files are confidential unless they have been explicitly made available to other authorized individuals.

(d) "Sensitive Information" may be either public or confidential and requires a higher than normal assurance of accuracy and completeness. Sensitive information requires special precautions to ensure integrity and to protect it from unauthorized access, modification or deletion.

3. Responsible Use. As a learning organization, it is within the scope of responsible use to utilize College information resources, including e-mail, for personal and professional development activities, subject to the provisions that these activities: 1) do not interfere with college operations, 2) do not interfere with the ability of an employee to meet all job expectations, 3) do not unduly interfere with ability of other students to accomplish coursework, 4) do not impose a burden on College resources, and 5) are not among the prohibitions listed in Section 4 below.

4. Prohibitions. The following activities are specifically prohibited by this policy:

(a) Use of College information resources to originate, view, disseminate, or store material that: is libelous; violates copyright or other intellectual property law; intimidates, threatens, or harasses individuals or groups in violation of law or College Policy; endangers the security of information resources; or violates other state or federal law or College Policy.

(b) Use of College information resources in the operation of a commercial business or service. Exempted from this prohibition is the occasional posting of articles for sale on electronic "bulletin boards."

(c) Use of College information resources to gain access to sensitive or confidential information which is not required to perform job duties.

(d) Attempting to circumvent system guidelines or security or invade the privacy of individuals.

(e) Deliberately attempting to degrade the performances of a computer system or information resource; damage hardware, software or data; or to deprive authorized personnel of resources or access to any College computer system.

(f) Allowing another to use an assigned authenticated user account or using the authenticated user account of another individual without appropriate prior supervisory approval. Specifically prohibited are:

- revealing passwords either verbally or in writing;
- negligent disclosure of passwords such as posting passwords on or about workstations; and
- attempting to learn the password of another user

(g) College authorized users may not attempt to repair or modify hardware that is under warranty agreement and that is part of the College hardware inventory, without the express written permission of the manufacturer.

(h) Users may not duplicate licensed software or related documentation for use either on College premises or elsewhere unless the College is expressly authorized to do so by agreement with the licensor.

(i) Users may not download or install non-college standard software to any college computing device. Users will not in general be given administrative rights to College-owned computers, whether the computer is a desktop or a laptop. *Users may not load games, entertainment software or personal finance software on a college-owned laptop computer. All Peer to Peer (P2P) file sharing software (such as Kazaa, Limeware, Bearshare, etc.) is strictly forbidden as they are notorious for attracting SPAM, spyware, malware and denial of service attacks.*

5. User Responsibilities:

(a) Users are responsible for adhering to all other college policies for use of electronic media including but not limited to; Social networking policies; Mobile Communication Devices; Laptop User Guides; and Computer Lab Procedures.

(b) Users will be held accountable for immediately notifying OIT department in the event they suspect a college-owned device or a personal device (which may include but is not limited to a mobile communication device such as a Blackberry, IPhone, IPod, IPad, other smart phone device, personal laptop, or USB key) carrying college data is in anyway compromised (lost, stolen, hacked, etc.)

6. Violations and Discipline. All College employees who violate this policy are subject to disciplinary action up to and including termination of employment. An employee who is subject to disciplinary action based on an allegation of a violation of this policy shall be entitled to full due process provided under the appropriate process.

All students who violate this policy are subject to disciplinary action consistent with the student handbook.

Violators may be subject to legal action.

7. Certification. All users, by accessing any College information resources are certifying that they understand and accept the provisions of this Policy and may be subject to disciplinary action for infringements of this policy. “Users” may be defined as students, employees or community members.