INSTITUTIONAL DIRECTIVE 2-10

May 14, 2007

Title: Use of Computers, Network Services, and the Internet

I. Purpose

The intent of this directive is to articulate the policy and procedures regulating access to and use of Piedmont Technical College's computers, network services, and the Internet by employees, students, and other authorized users.

II. Policy

It is the policy of Piedmont Technical College to allow employees, students, and (in special circumstances) members of the general public to use the college's computer resources (henceforth designated as the network); such use, however, must conform to acceptable requirements as defined by this policy and other relevant policies and by state and federal legislation.

III. Philosophy

Computer networks offer a powerful medium for communication, data storage, and information retrieval. Access to such systems, however, imposes certain obligations upon users. In a broad sense, these obligations are legally prescribed. They are further defined by specific agencies and institutions such as Piedmont Technical College. The college asserts both its right to formulate such policy and its insistence on compliance. Those who accept the privilege of using the network concomitantly agree to abide by the declared policy.

IV. Responsibilities

Authorized users of the college's network will:

A. Use it only for college business and access only those files and data that are their own, that are publicly available, or to which they have been authorized access. College business implies purposes that are related to instruction, research, or administrative management. "Official state business" for education and research purposes by entities established specifically for such purposes (e.g. schools, colleges, universities, and libraries) may be more broadly interpreted in accordance with guidelines developed by such entities.
B. Refrain from monopolizing or overloading the network through excessive data or time, disk space, printer paper, or other materials.
C. Protect network security and act to prevent any unauthorized use.

V. Procedures

To implement this policy, the following procedures will be observed:

A. Network access will be granted to specific employees, students, and other users as authorized by the administration of the college through user accounts or other means of identification as appropriate.

Office of Responsibility: President

B. Levels of technology (including software) will be assigned to individuals based upon particular job or educational requirements.
C. Use of the network for illegal or immoral purposes, or to support such purposes, is forbidden.
D. Use of the network to harass, intimidate, or annoy another person is forbidden.
E. Use of the network for private, recreational, non-public purposes, including the conduct of personal commercial transactions is forbidden.
F. Use of the network for partisan political purposes is forbidden.
G. Use of the networks or other state equipment for personal gain such as selling access to any systems or by performing work for profit utilizing state resources not authorized by the State is prohibited.
H. Use of the network in such a way as to disrupt other users is forbidden. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer "viruses," and sustained high volume network traffic, which substantially hinders others in their use of the network.
I. Any attempt to circumvent or subvert network security is forbidden.
J. Interception of network traffic for any purpose unless engaged in network administrative duties is prohibited.
K. Attempt to access and/or duplicate copyrighted, proprietary, or otherwise restricted information or material as defined by State Board policy is forbidden.
L. Plagiarism from network sources is forbidden.
M. The display or duplication of any material that might be defined as obscene or pornographic is forbidden.
N. Users, who download information, should consider document size and time requirements for completing the process. (see Downloads Policy)
P. Users should protect their User ID, passwords and computer system from unauthorized use. Users should also be prepared to assume responsibility for any changes associated with billable services unless appropriate authorization has been obtained.
O. Users shall not make or use illegal copies of copyrighted software or other mediums, store such copies on state systems, or transmit them over state networks. State and Federal law prohibits the downloading music, videos or other copyrighted files without due process and express permission of the owning institution.

VI. Enforcement

The college reserves the right to monitor the content and volume of network traffic to ensure user adherence to this policy. Access to computer systems and networks owned or operated by Piedmont Technical College impose certain responsibilities and obligations on system users and is subject to state government policies and local, state, and federal laws. Violations will be managed as follows:

A. Faculty and Staff: Violators will be required to confer with their immediate supervisors who will take action as deemed necessary.
B. Students: Enrolled students found to be in violation will be asked to suspend the inappropriate network activity. Those failing to comply may be subject to discipline under provisions of the South Carolina Student Code.

C. General Public: Users from the general public who violate the policy will be asked to suspend the offending behavior. Failure to do so will result in revocation of network privileges.

In all circumstances, those users whose behavior violates established law will be subject to prosecution.

Original on File **5/14/07**
Approved for Publication **Date**

Downloads and Executables Policy

This policy has been established to set guidelines in an effort to clarify the type and nature of files that employees are allowed to download from third-party sources onto their local computers (desktops, laptops, Pocket PCs, Tablet PCs). Although it would be impossible to name every executable or download file in this policy, users should adhere to these guidelines:

1. The download enhances the employee's productivity.
2. The download is from a reputable source.
3. The file does not subject the company to potential liability.
4. The application, tool, or template has been approved by IS.

APPROVED DOWNLOADS

The following is a list of files that employees can download onto their local machines.

- **WinZip**

  Employees who e-mail large files to contractors and consultants are encouraged to use WinZip, a compression utility.

- **Ad-aware**

  As employees may unwittingly download adware onto their local machines, applications such as Ad-aware, which scans a user's system for adware, are allowed. Please note: Some useful proprietary applications on the company network are seen as adware by this and other similar applications. Contact the IS department if you have questions about this kind of application.

- **RealOne Player, Microsoft Media Player or QuickTime**

  Employees can use these applications to listen to music and view streaming media at their workstation. Users will take care not to adversely affect other workers and will, for example, keep the volume of the music and other media played on this application within reasonable levels, if they are located in an office. Employees are encouraged to use headphones if they work in cubicles.

- **Adobe Acrobat Reader, Adobe Reader**

  Users must have this downloaded to view PDF files.

- **Ebook applications**

  This includes Microsoft Reader, Palm Reader, and other third-party applications that allow users to download work-related texts onto their local machines.

PROHIBITED DOWNLOADS

- Peer-to-peer (orP2P) downloads of music or videos for personal use.
- Google, Yahoo or other "task bar" programs which reduce the efficiency of the provided desktop computer.
- Games
- Programs or internet address links for any gambling program.

Disclaimer: This policy is not a substitute for legal advice. If you have legal questions related to this policy, see your lawyer.