COMPUTERS AND NETWORKS USAGE POLICY

Introduction 1:762

As a part of its educational mission, Andrews University provides data communications and computing services to University students, faculty, administration, and staff. The following policies and guidelines are established to maximize the educational benefit realized from the considerable investment of resources necessary to operate and maintain these facilities. Non-compliance with these policies and guidelines may result in penalties of varying degree. See Section 1:762:21 (A.1.11) for procedures for making an appeal.

A. General Guidelines 1:762:10

1. Providing and financing computing and data communications services on the Andrews University campus is shared by different groups and individuals: 1:762:11

    a. Information Technology Services (ITS) provides and maintains the university-owned data network and building connections, administrative and academic computing servers, email and Web servers, and general computing laboratories. ITS organizes additional services for the campus for which the consumers pay, including sales of computing hardware and software and installation and maintenance of university-owned computers and software.

    b. Administrative and academic departments budget their own resources for purchasing and maintaining their computing facilities and are encouraged to obtain the services through ITS.

    c. ITS sets policies for the installation and maintenance of standard and non-standard software packages on University-owned computers. These policies are described on the ITS-Client Services web site (http://www.andrews.edu/ITS/CS).

        To avoid duplication of administrative data and/or systems, to ensure data and network compatibility, and to maximize opportunities for technical support, all software that uses or interfaces to institutional data must be approved by the Director of Administrative Systems in ITS prior to purchase or development. The term "institutional data" includes data held at the school or departmental level as well as data on the central server. Schools or departments where a violation of this policy is found will be asked to convert to an approved system.

        To ensure compatibility with our environment, and the availability of on-campus support, schools and departments should consult with the Director of Client Services in ITS prior to the purchase of all other software.

    d. All students have access to computers and data communication through general and departmental laboratories on campus. Access to the campus network through direct or dial-up connections is made available to students with personal computers who live in University facilities. Help desk assistance and maintenance are not provided for student-owned computers unless they were purchased through ITS.

e. A limited number of dial-up lines are provided by ITS for the use of off-campus students and University employees. Although there is no charge for using these lines, availability is not guaranteed. University policies governing computing on campus apply to the use of these lines.

2. Individual access passwords should be carefully guarded, changed frequently, and treated as a signature, that is, not shared with anyone else including fellow employees or family members. **1:762:12**

3. Prohibited activities on campus computers and networks, some of which may constitute criminal activity, include but are not limited to the following: **1:762:13**

   a. Unauthorized access to or use of other users' accounts, system software, university data, or other computer systems.
   b. Unauthorized decryption of coded information such as passwords.
   c. Attempts to "crash" computers or network services.
   d. Storage or transmission of copyrighted materials without the owner's permission.
   e. Willful introduction of viruses or other disruptive/destructive programs.
   f. Attempts to evade or bypass system administration policies, such as resource quotas, firewall and web filter settings.
   g. Forgery or attempted forgery of documents or email.
   h. Excessive use of resources, such as network bandwidth or disk storage.
   i. Unsolicited "broadcasting" of email (spam or electronic junk mail).
   j. Generating or forwarding chain letters, or participating in any kind of multilevel or pyramid scheme.
   k. Harassment or intimidation of other users, including sexual harassment.
   l. Accessing or downloading any kind of pornographic material.

4. Information transmitted over the network or made available to others (e.g. through Web pages or bulletin boards) should be representative of a Christian university. For example, materials -- text or graphics -- should not contain: materials characterized by profanity or obscene language; defamation of any individual or group; materials promoting hatred of cultural, ethnic, or religious groups; advocacy of lifestyles contrary to University policy; pornography and other sexually-oriented material. Illegal materials such as child pornography should not be accessed by or stored on any computer while connected with the University, whether private or University owned. **1:762:14**

5. Andrews University cannot guarantee the confidentiality or privacy of electronic mail messages and other documents stored on University computers, and the University makes no promises regarding their security. Such messages should be written with this in mind. The ease of saving, forwarding, and printing electronic mail messages and documents makes them more akin to formal letters and memoranda than to verbal communications. **1:762:15**

   The following guidelines relate to confidentiality:

   a. Andrews University reserves the right to conduct routine maintenance, track problems, and maintain the integrity of its systems. As is the case with all data kept on Andrews' computer systems, the content of electronic mail may be

revealed by such activities.

b. Andrews University does not routinely monitor the contents of email. However, such monitoring may be conducted when required to protect the integrity of the systems or to comply with legal obligations. (amend to cover SPAM filtering)

c. Andrews University reserves the right to inspect the contents of electronic mail and all disk files in the course of an investigation into alleged impropriety or as necessary to locate substantive information not readily available by other means.

d. Authorization to investigate the contents of user files must be given by the Chief Information Officer on the basis of instructions from the University Administration.

6. Because unlocked computers are not insured, every effort should be made to preserve the physical security of personal computers. For example, a physical locking device and locking access doors (where applicable) should be maintained. Portable computers should be under personal supervision, in a locked space, or secured with a locking device at all times -- especially when traveling. **1:762:16**

7. Users are responsible for the security of data on their personal computers. Where sensitive information is stored on a personal computer, access to internal storage should be limited by a password. Centralized backup may be implemented for some personal computers; for all other machines, the user should carry out regular backups onto removable disks or tapes. Storage media containing sensitive information (backup or otherwise) should be kept in a locked space. A personal computer connected to sensitive information (local or through the network) should not be left unattended. **1:762:17**

8. University-owned personal computers are to be used for University business. In computing laboratories, academic work of students and faculty takes precedence over personal uses. Use of University computers for personal commercial activities is prohibited. The dial-up lines may also be used for personal communications, but other University policies apply, and available resources may restrict personal use. Employees' use of games on University-owned personal computers is prohibited during work hours except where an academic or administrative objective arises. **1:762:18**

9. "University work" should generally be done on computer or communications equipment provided by the University. Where personally owned equipment is used for University business, the University assumes no obligation to maintain or replace this equipment unless arrangements are made in advance. **1:762:19**

10. Andrews University will, as needed, filter objectionable email such as unsolicited commercial email, email spreading viruses, and email containing inappropriate references to pornography. Decisions regarding the methods and criteria to be used to filter email shall be made by the Chief Information Officer (CIO) or his/her designee and communicated to the Academic and Administrative Computing Committees. (move to section C. Email & Web) **1:762:20**

11. Appeals to decisions made regarding any Computer and Networks Policy shall first **1:762:21**

be taken through the appropriate managerial levels up through the CIO. Issues that cannot be resolved through this method may be brought to an ad hoc appeals committee composed of three members from the Academic Computing Committee and three members from the Administrative Computing Committee. This ad hoc committee shall have authority to reverse decisions made and recommend policy changes. The appeals committee shall elect its own chairperson. The appeal process begins with a request to the chairperson of either computing committee.

B. Networking And Data Communications 1:762:30

1. The University provides a data network connection for most computers connected with the University. This connection gives access to other computers and services both within and outside the campus. Every employee and student can request an account on at least one central computer to permit access to email, the World Wide Web, and other local and national/international services. ITS takes steps to protect server-based user files from unauthorized access from on or off campus. It is the responsibility of the user to protect locally stored files. (amend to cover single logon – terminology?)

2. In cooperation with various campus committees, ITS sets technical and operational standards for data networking and computing on campus. Anyone connecting a computer to the campus network – student or employee – is required to abide by the standards set by ITS. In addition, help desk assistance is available only for software on a supported list. **1:762:31**

3. Connections to the campus data network may be made or changed only by personnel from ITS. **1:762:32**

4. No unauthorized name servers are permitted on the campus network. **1:762:33**

5. Any service that is provided outside the University by a computer on the campus network requires the approval of the Chief Information Officer. Examples of services include web, mail, FTP, telnet, games, bulletin boards, discussion groups, interactive chat services, streaming media. **1:762:34**

6. Any computer on the campus network that is configured to be a server must permit administrative access by University network administrators. From time to time, University network administrators will make arrangements with departmental server administrators and their users to determine the level of vulnerability to attack by hackers or other threats to security or service. Servers found to be vulnerable will be required to be brought into compliance or be removed from the Andrews network. **1:762:35**

C. Email And Web 1:762:40

1. Widely accepted etiquette for the Internet and Web should always be observed. For example, email should not be sent to users, lists, or newsgroups where the subject is not appropriate, where the email is not welcome, or the document size or number of destinations is excessive. **1:762:41**

2. University employees and students may set up a home page on the World Wide Web containing personal as well as University information. Such pages must follow guidelines established by the Web Committee. The owner of a Web site is responsible for the content of all pages in the site that are on computers connected to the University network and for all first-level links from these pages. **1:762:42**

3. Andrews University will, as needed, filter objectionable email such as unsolicited commercial email, email spreading viruses, and email containing inappropriate references to pornography. Decisions regarding the methods and criteria to be used to filter email shall be made by the Chief Information Officer (CIO) or his/her designee and communicated to the Academic and Administrative Computing Committees. (moved from 1:762:21) **1:762:43**

4. Inbox policies

D. Software And Intellectual Property 1:762:50

1. All software on University or personal computers, whether on campus or connected to the campus network, must be legally licensed by the owners of the software or copyrights. Users must observe license and copyright restrictions of all software and documentation. Usually this means that commercial software may not be copied to other machines and that documentation should not be copied. The University will purchase "site licenses" for selected widely used programs. ITS personnel must install these programs, and users may not copy or move them to other machines. Users may install other copyrighted programs on personal computers provided an appropriate license has been purchased. Many software packages are available at academic discounts through the University Bookstore. **1:762:51**

2. Copyright laws should be observed for documents (text, graphics and all multimedia) as well as for computer software. (A summary of the copyright law appears in Appendix RR.) **1:762:52**

For example, copyrighted materials should not be used in Web pages (departmental or personal) or instructional materials unless the use falls under the educational "fair use" clause as defined by the United States Copyright Act. (Appendix SS includes a definition of "fair use".) The following resources on the Web may be helpful to users in deciding whether a particular usage of copyrighted material qualifies as a fair use:

http://www.utsystem.edu/OGC/IntellectualProperty/copypol2.htm#test
http://www.benedict.com/fairtest.htm

In addition to fair use, copyrighted material may also be used if the material lies in the public domain. Items in the public domain (for example, items for which copyrights have expired) are no longer subject to copyright and do not require permission from the copyright owner. For more information on public domain works, consult the following Web site:

http://www.unc.edu/~unclng/public-d.htm

The following Web resources may be helpful to users with questions regarding copyrights:

http://www.spa.org/piracy/highered
http://www.utsystem.edu/OGB/IntellectualProperty/cprtind
http://www.benedict.com/webiss.htm
http://www.fplc.edu/tfield/copynet.htm
http://fairuse.stanford.edu