

Network Policy

Computing and Information Services- Fred Miller, Chief Information Officer

Title: Network Policy

Applicable: Furman University (Students, Faculty and Staff)

Contacts: The Computer Help Desk ext.3277

Background: Furman University provides a campus computer network, including access to the Internet, for Students, Faculty, and Staff, in order to conduct official University business and to further the educational purposes of the University. Use of the Furman University network is governed by this Network Use Policy and is subject to all applicable federal, state, and local laws as well as the rules and regulations of the University.

Policy: The primary purpose of the University's network is to support University business and academic endeavors. Beyond these primary functions, all users of the Furman University network will generally be granted equitable access to as many network services as technology and network capacities allow. University Faculty, Staff and Students that wish to use the campus network must adhere to the following Guidelines. Guidelines:

1. The University respects the fundamental privacy of electronic communication on the campus network. The University does, however, reserve the right to gain access to otherwise private network correspondence or files maintained on the campus network. Such access might occur in certain specific circumstances such as where a possible violation of the Network Use Policy is investigated in order to protect the security, integrity and effective functioning of the campus network or Furman University's interests. System administrators may require access to otherwise private files maintained on the campus network to comply with certain situations such as University and law enforcement investigations, legal requirements, or as part of regular system maintenance. An attempt will be made to notify the user of this access in advance whenever possible and appropriate. Such access is governed by applicable federal, state, and local laws.
2. Furman University encourages a free and open forum for personal expression. This includes viewpoints that are unorthodox or unpopular. Except for official statements from appropriate University officers, Furman University does not officially endorse any opinions stated on the network.
3. All members of the University community are encouraged to communicate differing perspectives. Community members are also, however, entitled to work and live in an environment free of harassment. Therefore any network activity that violates the University's harassment policy is prohibited. Defamatory remarks and obscenity are also prohibited. The use of overt profanity is strongly discouraged.
4. Access to the network is through individual accounts with password protection. All willful violations of this policy that can be traced to an individual account name will be

treated as the sole responsibility of the owner of that account.

5. The running of programs, services, systems, processes or servers by a single user, or group of users, that may substantially degrade network performance or accessibility will not be allowed. Electronic chain letters, mail bombs, and excessive recreational use of the network are prohibited.
6. Individuals may not place any type of personal networking equipment on the Furman network without the express permission of the Chief Information Officer of Computing and Information Services.
7. Computing and Information Services will not share, or support the sharing, of any printer on the network from a desktop computer, unless the printer is a legacy device. To install a printer on the network, it must have a network card and be capable of obtaining its own IP address.
8. Computing and Information Services will not share, or support the sharing, of any file or directory on the network from a desktop computer.
9. Furman University expects its users to comply fully with United States and State of South Carolina copyright law and with the Digital Millennium Copyright Act (the DMCA).
 - a. Computing and Information Services is not responsible for policing or obtaining permission of copyrighted material; it is the responsibility of the group entering the content to obtain the appropriate permissions. All electronic content placed on the network is subject to this policy, including but not limited to University web servers, network shares, The Digicenter and the document imaging project.
 - b. The use of file-sharing programs such as KaZaA, and peer-to-peer (P2P) technologies to download and/or share copyrighted music or other content is illegal. Members of the Furman community are prohibited from downloading or sharing copyrighted material without license to do so, and are prohibited from storing copyrighted material, even if as a personal archive, on unsecured network areas.
 - c. Content discovered through routine scans of the network by Furman's system administrators that appears to be copyrighted media may be removed.
 - d. Notices of violations discovered by recording or movie industry sources received by Computing & Information Services and involving students will be referred to Student Services for disciplinary action. The illegal downloading or sharing of copyrighted media may result in fines, the loss of access to all network resources at Furman, or criminal prosecution.
 - e. Network community members must respect all copyrights and always provide proper attributions of authorship. Commercial software licensed to Furman University may be installed only on machines expressly covered by the licenses. Upon request from a network administrator, individuals who have software licensed to them and installed on a Furman University computer shall produce original disks and/or documentation to verify compliance.
 - f. If you download any audio or video content, be sure you are entitled to do so. Then protect yourself by storing appropriately obtained media in a private, secured area. Be aware that some file sharing programs such as KaZaA may set up open sharing on your system without your knowledge

when you install them. You are responsible for sharing that occurs on your computer whether or not such sharing is deliberate.

10. Users should only download audio or video content to which they are entitled. Users that download appropriately obtained media should protect themselves by storing that media in a private, secured area. Be aware that some file sharing programs such as KaZaA may set up open sharing on systems without the knowledge of the user. Users are responsible for sharing that occurs on their system whether or not such sharing is deliberate.
11. Network users are expected to use network printing in a responsible manner by printing only those materials essential to educational, academic, or University needs.
12. Approval from the University's Chief Information Officer is required before any member of the Furman University user community may install or use any remote access software or any server software on any computer connected to the Furman University network.
13. Without specific authorization, users of the Furman University network must not cause, permit, or attempt any destruction or modification of data or computing or communications equipment nor remove or aid in the removal of any Furman University-owned or administered equipment, data, or documents from the Furman University network.
14. Employees of Computing and Information Services may make appropriate changes to any computer connected to the Furman University's network consistent with the Network Use Policy, or when necessary for maintenance or repair.
15. Deliberate attempts to degrade or disrupt the system performance of the Furman University network or any other computer system or network on the Internet by spreading computer viruses, worms, or similar programs is considered criminal activity under state and federal law. As a precondition for network attachment and use, all personal computers must have up-to-date virus protection software installed and operating.
16. Impersonation, anonymity, pseudonyms, spoofing, and other methods of hiding, intended to cloak the true identity of a user in order to mislead or avoid detection, is prohibited.
17. Identity theft, including improper or unauthorized use of another person's electronic mail account, credit card, PalaCard, residence hall room telephone, cellular telephone, or any other private possession, is strictly prohibited. (An additional charge of theft may be imposed when appropriate).
18. The use of the University network and/or University hosted web pages to offer goods or services of a business or commercial nature is not permitted except those consistent with the University's educational or business mission.
19. Use of the University's network for any activity contrary to local, state, or federal laws is prohibited. Illegal activities include, but are not limited to, tampering with computer hardware or software, unauthorized entry into computer systems or computer data, willful vandalism or destruction of computer data or files, or any attempt to defeat the Furman University computer or network security systems.
20. Users should report any knowledge or evidence of violations of the Network Use Policy to the Computer Help Desk or to the University's Chief Information Officer. Incidents of harassment should also be reported to the University's Chief Information Officer.
21. Reported violations will be investigated. If the investigation yields substantial evidence of a violation of the Network Use Policy, the case will be heard through the normal University processes for reviewing a violation of policy.

22. Students who violate the Network Use Policy may be subject to the full range of sanctions as set forth in the Penalties section of the Helmsmen, including, but not limited to, possible suspension or termination of network privileges. Other users who violate this policy will be subject to sanctions and/or network use limitations as determined by the University's Chief Information Officer, or other appropriate University official. Computing and Information Services has the authority to temporarily revoke network access or take other appropriate action in order to maintain network security or health until the investigation of the alleged infraction of the Network Use Policy is complete.