

# Summit Christian College

## Computer Network and Internet Regulations

To ensure better quality network service, provide a safer learning and living environment, and to assist students and staff in personal purity, the following regulations are adopted as of January 16, 2004. Many of these new rules are merely an expansion of existing policy, while others, such as file sharing, needed to be addressed because the amount of bandwidth that it requires is slowing the entire system and very often Internet users do not realize that it is an illegal activity.

1. Users of the Summit Christian College computer network must exercise integrity of character while using the network.
2. Unless specifically authorized by Summit Christian College Administration or Board of Trustees, the following is strictly forbidden:
  - a. Using an account other than your own to obtain unauthorized access to accounts or information on the school network connected to the Internet.
  - b. Attempting to gain access to restricted sites, servers, databases, etc.
  - c. Attempting to harm or destroy the data of another user, agency, or network connected to the network or Internet.
  - d. Degrading, disrupting or damaging network equipment, computers, software or system performance.
  - e. Changing settings, including screensaver and desktop settings, on public computers, printers, scanners or other peripherals.
  - f. Use of the network for pirating software, data and music files on personal computers, printers, scanners or other peripherals.
  - g. Wasting network resources, including network bandwidth, server storage capacity, and printer supplies.
  - h. Accessing, storing or printing files and images which are threatening, profane, obscene, degrading, or blasphemous.
  - i. Using the Internet to create, publish or distribute threatening or profane material.
  - j. Distribution of copyrighted material, or any activity prohibited by federal, state or local law.
  - k. Using the Internet or network for plagiarism.
  - l. Downloading and/or installing software of any kind on public computers. This includes but is not limited to, video games, chat rooms, Internet games, audio files, video files, MP3 players or files, messaging clients, e-mail clients, or any software that modifies the computer's configurations.
  - m. Students sharing personal network account information with other students.
  - n. Use of file sharing programs such as BitTorrent, Napster, Kazaa, Gnutella, Share Bear, Limewire, etc.
3. Staff and students are assigned an IP address when their computer is registered into the network. All users are responsible for whatever happens on their workstation. Users should configure their own computers with personal settings to deny unauthorized use by other staff, students or campus visitors. All users should not leave their workstation unattended without first logging off the network.
4. Users suspected of misuse may lose access to the Internet, access to the school network, and/or any school computer equipment. Additional disciplinary procedures will be implemented per the Summit Christian College personnel handbook.
5. Users are strongly cautioned against opening files from unknown sources, as it may contain a computer virus. Users are also cautioned about spreading rumors of viruses or forwarding suspicious files that may contain a virus or hoax.
6. Each user is provided with a network user account. Although user home directories are backed up on a regular basis, SCC I.T. is not responsible for the contents of these directories. Users must provide their own USB Flash Drive for back up.
7. Public computers are provided for research, and as a means for students without personal computers to compose their classroom assignments. Students with legitimate work have priority over those without.
8. Minor students will be blocked from Internet use if so requested by their parent or guardian.
9. The network traffic, both incoming and outgoing, is randomly reviewed for signs of inappropriate use. If a user should accidentally access a prohibited site or be sent a bad file, he or she should contact the administration immediately to avoid suspicion.
10. Students and staff should use the network in a manner that reflects appropriate use of their classroom time.

# New and Returning Student System Access Request

Last Name: \_\_\_\_\_  
First Name: \_\_\_\_\_

\_\_\_\_\_  
Last Name

\_\_\_\_\_  
First Name

I have my own computer that I would like activated on the network.

My computer's MAC address is:

--	--	--	--	--	--

I have read and understand the Computer Network and Internet Regulations. I understand that failing to abide by these rules may result in my being disconnected from the network and/or disciplinary actions being taken.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Office Use Only			
Username			
IP Address	192	168	
Completion Date			