

**Southern Connecticut State University**  
**Office of Information Technology**

**Acceptable Usage Policy**

The following is a set of guidelines governing the acceptable usage of computers, accounts, and network connections on the Southern Connecticut State University residential computer network. Access to and use of computing and network resources are privileges extended to residential students, but may be revoked based on failure to comply with these guidelines. The University reserves the right to amend these guidelines at any time, without prior notice, and to take further actions as may be necessary or appropriate to comply with local, state, and federal laws or University policies.

Most attempts to contact users concerning these guidelines will be made through their official University email address (MySCSU\_ID@southernct.edu) or by phone. All students are given University email accounts, but they may choose to forward it to another email system if they prefer. Any questions concerning the University email system should be addressed to the Help Desk @ 203.392.5123

**Antivirus Software:** Users are required to install antivirus software and configure it to update its antivirus definitions daily. The University provides excellent antivirus software that is available for free to all students. Failure to install or maintain antivirus software may result in removal from the network if your computer becomes infected with a virus. To download and install a copy of the University's free antivirus software visit <http://share.southernct.edu/swdist/>

**Authorized Access:** Do not give access to your computers, accounts, or network connections to other users, especially those not associated with the University. Users who knowingly give access to these resources to others will be held fully accountable for any violations of these guidelines that occur.

**Commercial Use:** Do not engage in any moneymaking activities with your computers, accounts, or network connections. This includes, but is not limited to, using email or hosting web pages to solicit a service, advertise a product, or conduct other types of non-University business.

**Copyright Policy:** Do not copy, display, or redistribute copyrighted materials, including software, music, and movies, except under limited "Fair Use" circumstances. This includes, but is not limited to, copying software that was not purchased, downloading a song that was not bought, or uploading a movie that was not made by the user. If the University receives a complaint that a user is redistributing copyrighted material that user's Internet connection will be blocked until the complaint is resolved. If the University receives multiple complaints about a single user their Internet access will be permanently disconnected and they will be referred to the University disciplinary system for appropriate action.

**Disruption of Service:** Do not deny any other member of the University access to their computers, accounts, or network connections. This includes, but is not limited to, deleting another user's system files, changing another user's account password, or disrupting network service with excess traffic or any type of attack.

**Harassment:** Do not harass another user with your computers, accounts, or network connections. The Southern CT State University's Policy on Harassment "forbids harassment that has the effect of interfering with an individual's performance or creating an intimidating, hostile, or offensive environment". This includes, but is not limited to, sending threatening email, setting up websites that sexually harass anyone, or continually sending unwanted chat messages to another user.

**Identity Theft:** Do not impersonate another user or conceal your identity when using any computers, accounts, or network connections to interact with official representatives of the University. This includes,

but is not limited to, forging email, creating fake accounts, or misidentifying yourself in official communications. Users may identify themselves by an alias to protect their identity on the Internet, but should reveal their identity when asked to by a University official.

**Passwords:** Do not share your passwords with another user, and password-protect shared folders and files. Sharing files without password protection allows others on the Internet to access them, and can allow others to use your computer to store their files. This includes, but is not limited to, telling someone a private password, not password protecting shared folders, and running ftp sites that allow anonymous access.

**Privacy:** Do not purposefully invade the privacy of another user's computers, accounts, or network connections. This includes, but is not limited to, intercepting another user's email, accessing another user's computer without their permission, or analyzing network traffic. The University monitors and records limited information from all network traffic to ensure the stability and security of the entire network.

**Registration System Abuse:** Users who abuse the network registration system by changing their network hardware address, stealing an IP address, or otherwise modifying their network information with the intent to deceive will be immediately and permanently disconnected from the network. Users disconnected for this reason are in danger of losing their housing and will be referred to the University disciplinary system for appropriate action. Users are expected to allow DHCP to automatically configure their computer's IP address - usage of static IP addresses is prohibited and will prompt an investigation into their network usage.

**Wireless Access Points:** Users who wish to operate wireless access points should be aware that they are responsible for all traffic that passes through that access point, including but not limited to bandwidth usage, copyright abuse, virus infections, harassing or threatening messages, and all other network usage. Improperly configured access points can cause interruptions on the network and will be immediately disconnected from the network.

In addition to these guidelines, users must abide by the rules and regulations of the Universities "Policy on Computer Use & Software Guidelines", the Dean of Student Affairs "Student Handbook", and all other applicable University policies and local, state, and federal laws. If the University is contacted by a local, state, or federal law-enforcement agency concerning any user's activity on the network full cooperation is required.

It is implied that all users inherently accept this policy. By accepting this policy, users of the residential computer network agree to follow all listed guidelines. Any violation of these guidelines may be subject to disconnection from the network, disciplinary action, and/or legal action by the University and/or local, state, or federal agencies.