

ResNet Acceptable Use Policy (AUP)

v. S03.2009

You are responsible for/understand that:

- Your devices connected to the campus network, including ResNet and wireless
- Registering for your connection. Every computer that connects to the residential network (ResNet) must be properly registered with ResNet and be properly configured for the network. This includes installing the ECU version of Symantec Antivirus, Cisco Clean Access, and all Microsoft Windows/Apple Macintosh Updates and Service Packs.
- All network activity originating from your equipment. Every bit of information that comes from your computer, whether you generate it or not, is your responsibility. The use of ECU's network is a privilege, not a right.
- Protecting the privacy of your accounts. Don't release your personal account info to friends, relatives, roommates, etc. Likewise, don't ever use a computer account that you are not authorized to use or obtain a password for a computer account not assigned to you.
- Ensuring the security and integrity of your computer system. This includes (1) virus and spyware protection; (2) data backups; and (3) physical security.
- To connect other devices (game consoles, TiVo, etc.) to ResNet you must use the wired Ethernet in your room and bring us the device's MAC address to register it (Combs 230).
- Your agreement to all computing systems also covers the Code of Ethics for Computing & Communication (available at: <http://www.itds.ecu.edu/codeofethics>) and all local, state and federal laws.

Section I: Terms and Conditions

Carefully read these policies. These policies describe the acceptable use of ResNet at ECU. This is an official agreement that each student undertakes when registering for/connecting to ResNet service. By connecting to ResNet you agree to abide by this AUP.

The use of this service is a privilege because you do not own your account. You have exclusive access to this account given to you by ECU. It is the responsibility of the user to abide by the following guidelines, which are intended to preserve the utility and flexibility of the system, to protect the work of students, and to preserve the right to access the international network to which ECU systems are connected. Failure to comply with these guidelines will result in, at minimum, termination of service. Cooperation will protect your connectivity and your academic career.

Note: As long as you act responsibly by being careful, honest, civil, and complying with all laws and regulations regarding computers and networks while connected to ResNet, or any other computing service at ECU, you shouldn't have problems.

Section II: General

The residential network (ResNet) is a shared resource and is just a small part of the entire ECU network system. It exists to support the educational mission of our students and its use should be limited to this purpose. Network use or applications that inhibit or interfere with the use of the network by others are not permitted. (For example, using an IP address not registered to you or applications which use an unusually high portion of the bandwidth (e.g., KaZaa, BitTorrent, Limewire) for extended periods of time, thus inhibiting the use of the network by others, are not permitted).

Section III: Privacy

Users must recognize that there is no guarantee of privacy associated with their use of University network and computer systems. Network data to and from your in-room connection is monitored by IT. They perform monitoring in order to try to protect the network and users from viruses, hackers, and other malicious attempts to compromise the security of ECU's computing infrastructure.

The University may find it necessary to view electronic data and it may be required by law to allow third parties to do so (e.g., electronically stored data may become evidence in legal proceedings). It is also possible that messages or data may be inadvertently reviewed by others.

Section IV: Authorized Use

An authorized user is any person who has been granted authority by the University to access its computing

and network systems and whose usage complies with this policy. Authority to use a particular University computing or network resource should come from the campus unit responsible for operating the resource. Unauthorized use is strictly prohibited. The term "authorized user," "user," and "student user" are hereinafter used interchangeably.

E-key. University supplied E-keys (usernames and passwords) are the property of the University. The University may revoke these identifiers or sign-ons at any time. Default passwords should be changed immediately. Passwords associated with an individual's E-key should not be shared without authorization. Compromised passwords may affect not only the individual, but also other users on campus or on the Internet.

You are responsible for any activity linked to your e-key.

Passwords. Make sure all passwords are at least 8 alphanumeric characters long. Use a different password for each account. Don't write them down or share them with anyone. Change them ever 3-4 months.

NOTE: EKU, or any other reputable business/organization, will never ask for your personal information (username, password, account information, financial information, EKU ID number, Social Security number, etc.) in an email!!!

Attachments, Links and Popups. A lot of the malware (viruses and spyware) contracted today are a result of these three common issues from emails, instant messengers, chat programs, and social networking websites such as Facebook or MySpace.

Unless you're waiting on and expecting an attachment or a link from someone—DO NOT OPEN OR CLICK ON IT. This is a very common way for malware to spread.

Another common spreading tool involves pop-ups—even if you aren't actually "on" the Internet. These programs usually masquerade as "legitimate" software such as spyware or virus removal programs, registry cleaners, or codecs. They make exaggerated claims about your computer safety so you will install them. But they are, in fact, viruses and spyware!

Section V: Private Computers Connected to the University Network—Prohibited Activities

To maintain network performance, the conditions listed below are strictly prohibited. Note that many of these activities are caused by inaction, not action.

- Use of network for commercial purposes
- Host data services for other people or groups
- Share the network connection beyond your own use
- Deceive others about your identity in electronic communication or network traffic
- Attempt to access accounts, files, or information belonging to other users without their knowledge and explicit consent
- Use your network connection to threaten, intimidate or harass others
- Use your network connection to engage in any form of illegal software sharing, file sharing, copying, or engaging in any way in other types of copyright infringement
- Any intentional or unintentional action that impairs the overall functions of the network
- Any intentional or unintentional action that would deny or impair network service to another system or user
- Any intentional or unintentional distribution of computer viruses and other malware
- Operation of unauthorized servers
- Operation of any service that makes unusually high demands of the network
- Any action that violates Federal, State or University policy or law
- Scanning any system(s) or network(s) other than the computer(s) registered to you
- Unauthorized installation of networking hardware (hub, router, wireless router)

Section VI: Required Software Policy

EKU supplies all students with an antivirus software that you must use while connecting to the campus network. This means that you will need to uninstall your current non-EKU antivirus and install ours. This program is free plus we update it for you as long as you're connected to the ResNet connection in your residence hall. We do this to protect your computer and our network.

You must also keep your operating system (Microsoft Windows or OS X) up-to-date. This also helps keep your computer and our network free from malware.

ResNet also provides users with Cisco Clean Access. This program helps block unauthorized users from using your network connection to access the network. Plus it will alert you of software security issues you need to address to gain access to the network.

Section VII: Software Licensing Policy

ResNet also provides users with malware removal programs.

All software that is not freeware is subject to licensing and must be properly licensed and all license provisions (installations, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to. Eastern Kentucky University assumes no responsibility for the licensors or maintenance of the software contained herein. The licensing is the responsibility of the user.

Copyright violation is subject to disciplinary action by the University and/or civil or criminal liability.

Federal law prohibits the transmission (sharing) of copyrighted materials without express written permission from the original copyright holder. Copyrighted works (including, but not limited to, original writings, software, movies, music, video games, and TV shows) may not be shared on the local network without written permission of the copyright holder.

Section VIII: Network Monitoring and Blocking

To keep the network running properly, the network is constantly monitored for vulnerable computers, infected computers, and abuse.

In some cases it may be necessary to immediately block network connectivity to your computer. For this reason, ResNet reserves the right to block network access to/from your machine without warning.

Section IX: Damages & Penalties

The student subscriber will be assessed a fee based on time and material for the repair of any damage to University facilities (ResNet wiring, hardware and/or jacks) with a minimum charge of \$100 per incident.

Failure to comply with any of these policies may result in termination of your ResNet service and/or criminal prosecution.

Residential Networking reserves the right to terminate any ResNet connection without notice should it be determined that network traffic generated from said connection drastically inhibits or interferes with the use of the network by others.

Section X: Enforcement of this AUP

Violations of this AUP will be adjudicated, as appropriate, by ResNet, IT, Office of Student Rights and Responsibilities, and the office of Student Affairs. Sanctions as a result of violations of these regulations may result in any of the following:

- Loss of University computing privileges;
- Disconnection from ResNet;
- University judicial sanctions (<http://www.studentjudicial.eku.edu/>);
- Monetary reimbursement to the University or other appropriate sources;
- Reassignment or removal from University housing and/or suspension or expulsion from the University;
- Prosecution under applicable civil or criminal laws.

Reports of problems or violations can be made through the ResNet office.

You can expect that your use of the ResNet system is private UNLESS there is a problem expected with your or other systems. Then "authorized" staff may look at any information or files necessary to solve system problems and to protect the system and the information it contains.

EKU Judicial Sanctions #19: Interfering with the use of or abusing any part of the University computing services or facilities. Penalties and sanctions range from a reprimand to expulsion.

Judicial sanctions relating to computer violations are available:
http://www.studentjudicial.eku.edu/computer_violations.php

Section XI: Abandonment of Personal Property

The Department of Residential Networking (ResNet), without liability, has the right to assess a packing and storage fee of any abandoned property left on the premises thirty (30) calendar days after the ticket was resolved. We have the right to dispose of any abandoned property left on the premises sixty (60) calendar days after the ticket was resolved. Personal property left in the ResNet offices after the ending ticket date shall be deemed to have been abandoned and will be removed and disposed of at the resident's expense. The University shall not be responsible or liable for any losses of or damages to any abandoned property.

Section XII: Waiver of Liability

In consideration of the service provided by the University hereunder, I assume all risks of connecting my equipment to the University system, and agree that neither Eastern Kentucky University nor any of its employees, officers, or agents shall be liable for any claims, demands, actions, or causes of action of any sort whatsoever resulting from personal injury (including death), property damage, or economic loss, including incidental or consequential damages, suffered or incurred to me arising out of my use of the services provided hereunder. I do hereby forever release and discharge Eastern Kentucky University, its trustees, officers, employees, agents, or servants from all such claims, demands, actions, or causes of action.

The University retains the right to make modifications to its ResNet regulations and sales/service/rates at any time. By accepting this agreement you accept any changes to this document while still connected to ResNet.

This contract is canceled automatically when the resident ceases to be an EKU student.

NOTE: This Acceptable Use Policy incorporates and supersedes any previous EKU ResNet AUP.

Last Update: 7/15/09

© 2009 EKU ResNet

