



MacMurray College

Residential Network Acceptable Use Policy

MacMurray College – Residential Network Acceptable Use Policy

Contents

| | |
|---|---|
| Responsibility | 3 |
| Hacking and Port Scanning..... | 3 |
| Security and Privacy | 3 |
| Server Services | 4 |
| MP3 Music, Movies and other Copyrighted Files | 4 |
| Domain Names..... | 4 |
| Routers and DHCP Servers | 4 |
| Network Traffic and Bandwidth..... | 4 |
| Misconfigured Services or Virus Infected Computers..... | 5 |
| Commercial Use | 5 |
| Anonymous Mailers | 5 |
| Intentional Abuse..... | 5 |
| Dynamic Document..... | 5 |

MacMurray College – Residential Network Acceptable Use Policy

MacMurray College provides computing resources and worldwide network access to members of the College's electronic community for legitimate academic and administrative pursuits to communicate, access knowledge, and retrieve and disseminate information. All members of the Mac community (faculty, staff, students, and authorized guests) sharing these resources also share the rights and responsibilities for their use.

Responsibility

Users are responsible for all traffic originating from their computer, including user activity, regardless of whether or not

- they generated it;
- they know what they are doing, and;
- they realize that they have violated any specific policies.

It is REQUIRED that all computers on the Residential Network have the following:

- anti-virus and spyware protection that is kept updated.
- the latest Microsoft Updates, if you are running Windows.

It is RECOMMENDED that all computers on the Residential Network that are running Windows operating systems

- change the Administrator Account to another name and use a strong password with both numbers and letters.
- disable the Guest Account.

In most cases, unintentional violations will result in a temporary loss of connectivity pending the resolution of the problem and education of the user. Repeat violations may result in a longer term or permanent loss of connectivity. In some cases, especially those in which the Computer Use Policy has been violated, further action may be taken.

All IP addresses within housing are assigned through an automatic process. **Under no circumstances may computers be configured with a static IP address.** Using an IP address that you have not been assigned is grounds for losing your network privileges. If you use a static IP address, you will cause conflicts on the network which deprives other users of network services and/or make it considerably more difficult to diagnose network problems. Additionally, users may not mask the hardware address of their machines. Any computer that is found with a masked hardware address or one consisting of all zeros will be disconnected until it is reconfigured.

Hacking and Port Scanning

Any unauthorized attempt to access another computer is considered hacking. It doesn't matter whether the computer being hacked into is on or off campus. Any report received by the IT office that a computer on the housing network attempted to hack into or scanned the ports of another will result in the immediate disabling of the network connection until the matter is resolved. Some examples of hacking are: password cracking programs, port scanning on any computer that is not owned by the person doing the scanning and gaining access or attempting to gain access to another computer without the owner's permission. Port scanning is considered by the vast majority of network administrators to be a "hostile" act and a precursor to an actual hacking attempt.

Security and Privacy

Network traffic is considered private. Because of this, any "packet sniffing," or other deliberate attempts to read network information which is not intended for your use will be grounds for loss of network privileges. In some cases, the loss of privileges may be permanent. Note that it is permissible to run a packet sniffer explicitly configured in non-promiscuous mode (you may sniff your computer's packets). This allows users to explore aspects of networking while protecting the privacy of others.

Users are totally responsible for the security and integrity of their systems. In cases where a computer is "hacked into," it is recommended that the system be either shut down or be removed from the campus network as soon as possible in order to localize any potential damage and to stop the attack from spreading. In such cases, if the owner cannot be contacted in a reasonable time the network administrator reserves the right to disable the network connection.

MacMurray College – Residential Network Acceptable Use Policy

Once the owner is made aware of the situation and agrees to take reasonable steps to ensure that the computer is not compromised, network privileges may be restored.

Any computer with shared drives or directories that are password protected is considered private, even if others that do not own the computer know the password. **Accessing password protected directories without the express permission of the owner is considered hacking and may result in permanent loss of network privileges.**

Server Services

Mac's Residential Network is designed as a CLIENT network, and as such the use of servers is discouraged and will be carefully controlled. Computers running any type of server that uses excessive bandwidth will either be disconnected from the network or have their bandwidth limited. Examples of server services include, but are not limited to: Peer-to-Peer services (Ares, BitTorrent, Gnutella, KaZaA, DC++, Filetopia, etc); Web or IIS; FTP; Shoutcast; WAREZ; Chat; Gaming servers and mIRC chat servers, including file servers.

From time to time, it may be necessary to block or stop certain server services if they adversely affect the performance of the network, or if they become security threats.

Further, residents that are running any Peer-to-Peer (P2P) program that is creating excessive connections on the network may be disconnected without notice. Excessive connections are defined as any computer within the Residential network that has in excess of 500 connections at any given time to other computers off campus. It is not uncommon for certain P2P programs to connect to several thousand computers. Excessive connections cause problems on the network, degrades performance and efficiency of equipment, and causes slowdowns and lag for all residents.

MP3 Music, Movies and other Copyrighted Files

Be aware that copying and illegally distributing copyrighted material is a violation of Federal Copyright laws, and you could be arrested and prosecuted in a criminal case or sued in a civil case. MacMurray College in no way condones or encourages this illegal activity and will take action to terminate Residential Network privileges of any resident breaking College regulations, State, or Federal laws.

MacMurray College is obliged to cooperate with any criminal investigation regarding these matters. Please be aware that according to copyright law, you do not need to be making a profit to be prosecuted for distributing copyrighted materials such as movie or MP3 files.

If you are offering copies of copyrighted material by any means, you are in violation of the Federal Copyright Act. If you have copyrighted files on your computer that are not legal copies of materials you own, delete them. If you are distributing these files illegally by any means, stop now.

Domain Names

No computer connected to the campus network will be assigned a domain name.

Routers and DHCP Servers

No routers are to be connected to any portion of the residential or campus network. The use of popular small home routers (cable or dsl) is not necessary and they are not to be used. Any computer misconfigured as a router or set up for home networking that assigns IP addresses cause problems on the network and will be immediately disconnected. Equipment that acts as a DHCP server is strictly forbidden.

Network Traffic and Bandwidth

Residential connections to the campus network and to the Internet are provided to allow students to fully participate in the legitimate educational missions of MacMurray College. In general, we encourage individuals to provide useful, interesting, and inventive content to the Internet community, so long as it remains feasible for us to do so.

It may not remain feasible to provide unlimited connectivity for systems that are not strictly serving the College's missions. Because of this possibility, we reserve the right to regulate the flow of traffic on the residential network to ensure that all users receive a fair and equitable use of bandwidth. This may include Traffic Shaping and limiting or blocking certain types of network traffic. The College may also request that users reduce the amount of traffic being

MacMurray College – Residential Network Acceptable Use Policy

caused by their service or, where necessary, to remove such systems from the residential network. In all but extreme cases, we will contact the owner of the system before removing it from the network.

Misconfigured Services or Virus Infected Computers

There may be times when a computer is unintentionally misconfigured or infected with a virus that causes problems on the network. In order to preserve the best service possible for the majority of users, every infected computer will be disconnected from the network immediately. We will attempt to notify the owner of the system by electronic mail that the computer has been disconnected and why.

PLEASE ENSURE THAT ALL COMPUTERS ARE KEPT CURRENT WITH UPDATED VIRUS PROTECTION SOFTWARE. THIS IS ABSOLUTELY ESSENTIAL.

Computers will be allowed back onto the network after the owner notifies OIT via e-mail that they have reconfigured the computer or removed the virus and resolved the problem.

Commercial Use

Under no circumstances will any individual be permitted to use their network connection or computing privileges for commercial purposes. You may not advertise any commercial products. Any commercial use of College facilities is explicitly prohibited and is grounds for loss of residential network privileges.

Any computer that provides services for a commercial operation (e.g. a web site selling commercial products), provides services of a commercial nature (e.g. provides web services to Non-MacMurray users, whether or not a fee is charged), or has a domain name with a commercial designation (currently .COM or .NET) is explicitly prohibited from the campus network.

Anonymous Mailers

All electronic communications at MacMurray College must accurately identify the sender. Anonymous mail forwarders are prohibited. Running an anonymous mail forwarding service is grounds for removal from the residential network.

Intentional Abuse

Systems found to be intentionally running programs that disrupt network activity or attack specific computers on the network will be subject to immediate removal and disciplinary action.

Dynamic Document

Please understand that this is a dynamic document and subject to change. Every effort will be made to keep a current version on our web site. You will be notified, via your MacMurray e-mail account, of any significant changes.