

---

# RESIDENTIAL NETWORK (RESNET) GUIDELINES AND POLICIES

## ABOUT THE POLICY

We encourage you to bring your own computer to campus to enhance your experience at Grinnell College. We allow your system to connect to our wired and wireless network and provide network services if you bring your own computer to campus. The residential network (ResNET) and the campus wireless network are configured to manage personal computer connections. Both the Academic Computing Use Policies of the college as well as these ResNET policies govern the use of those network services. Any violations can result in the suspension of your ResNET access and/or a complaint filed with the college's Judicial Board.

Remember that you are ultimately responsible for all actions on your computer. If you let others use your computer, make sure you are aware of their actions. It is also your responsibility to install and maintain virus protection software and keep your system updated with security updates. A software agent is installed on your system when you first connect to our network which controls access. You will need to have valid network credentials to log into this gateway. If you have any questions about these policies, email Karen McRitchie [mcritchi@grinnell.edu] at ITS.

## RESNET POLICIES

- You are not allowed to run a business for profit or non-profit from the college network.
- You are not allowed to scan the computers and/or network for network information, devices or computers.
- You cannot provide a pass-through site to other campus hosts, or provide remote log in (e.g. telnet. SSL access) on your computer for anyone other than yourself.
- You cannot provide links to, post or distribute obscene or threatening material or anything deemed as inappropriate or illegal by Student Affairs, Information Technology Services, or applicable laws.
- Unauthorized access or disruption of a computer system or its services is a violation of our network policy. This includes the use of programs such as WinNuke, any sniffer or network monitoring software, Crack or any other software that is used to assist in the compromising of a computer system or user account.
- Misuse of your email account by participating in harassment including threats, obscenity or sexual harassment, or continued pursuit of a person who wishes to cease correspondence is a violation.
- Participating in a chain letter, internet schemes, and "mass mailings" to other students/faculty, are in fact a violation of campus computing policies due to it's burden on the mail system.
- Forgery, or misrepresenting one's self for the goal of sending harassing email anonymously is considered a violation.
- In accordance with college guidelines and/or court orders, files and transmissions may be subject to search and examination by system administrators or employees as required to protect users and the integrity of computer systems.
- It is illegal and a violation of policy, to enter or use a person's computer, account, password, data, and network folders without permission.
- You must configure your computer for DHCP which will automatically ensure that you are using the correct IP address. Manually configuring an IP address that is not assigned to you, may result in a permanent disconnection from the network. If the action is associated with a violation of law or other policy, this can result in further actions.
- Providing for download, copyrighted music files (MP3 or other formats), movie files, or games, through the network without authorization from the owner of the copyright is illegal. This is a violation of Federal Copyright Laws (U.S.C. Title 17). The Recording Industry Association of America (RIAA), movie studios and other "owners" of media rights, has the right prosecute any person violating this copyright law. Students who violate this law will not be given a warning. Connectivity privileges will be immediately suspended and compliance with the policy will be enforced.

- You must comply with any virus/security software requirements established for the proper function of the network and security of those using the network which will require you to install proper virus protection software and allow our network agent to be installed on your system.
- Do not display or distribute information about the network including its configuration, security practices and all other information that compromises users or network security.
- Do not register a ResNet or Grinnell College IP address with any other domain name.
- Do not use applications which inhibit or interferes with the use of the network by others. This includes applications that use unusually high portions of bandwidth for extended periods of time.
- Grinnell College's ResNet network services and wiring may not be modified or extended beyond the area of their intended use. This applies to all network wiring, hardware and in-room jacks.
- Wireless hubs are not allowed on the Resnet network. A 100MB wired connection is provided for your use along with wireless access in all residential rooms.
- Gaming devices are allowed on the network. You must provide the Ethernet address of the device and we will allow the device network access.
- iPhones, iPads, iPods, PDA devices will be allowed to use the wireless network. The device's mac address must be provided so that an exception can be entered to allow access. We do not support these devices, so service and connection issues are not resolved by helpdesk or ITS staff.