

# All College Computer and Network Use Policies

## All College Computer and Network Use Policy

When you are granted access to a shared computer system or computer network you become part of a community of users. The Ithaca College All College Computer and Network Use Policy applies to all users of College computers and network resources. Additional policies may also apply to specific systems (such as the Ithaca College Web Policy for information posted on the Ithaca College Web server). Questions about this policy should be addressed to the Director of Information Technology Services ([its@ithaca.edu](mailto:its@ithaca.edu)).

### **Individual use**

Your account and network connection (ResNet or office) are for your individual use. A computer account is to be used only by the person to whom it has been issued. You are responsible for all actions originating through your account or network connection. You must not impersonate others or misrepresent or conceal your identity in electronic messages and actions.

### **Respect the privacy and security of users and systems**

Unless information is specifically made public or accessible to you, you should assume anything on the network is private. Just because you may have the ability, through a loophole, someone's carelessness, etc., to access files, directories, or information that does not belong to you, you do not have the right to do so. Any attempt to circumvent computer, network or file security or to take advantage of security lapses is prohibited.

### **Do not disturb other users or abuse computer resources**

Disruptive and/or invasive actions using computer systems and networks are strictly prohibited. Examples of this include, but are not limited to, viruses, threatening or harassing messages, "spamming\*," packet sniffing, self-perpetuating programs, excessive volume of file transfers, network traffic or printing, and other programs, files, hardware, software, or actions that deliberately or unintentionally degrade or disrupt system or network performance, compromise or circumvent system or network security, or interfere with the work of others.

The use of network hubs, routers, wireless access points, or other devices designed to share your network connection with multiple computers or devices are expressly prohibited.

Individuals are required to take reasonable precautions to ensure that their systems are secure; this includes maintaining current virus detection software at all times on their system(s).

### **Respect intellectual property**

The use of campus computer resources, including ResNet, to share or distribute copyrighted material to others without the permission of the copyright holder is prohibited. This includes, but is not limited to, using peer-to-peer applications (ex: KaZaA) to share these files. The burden of proof of ownership or obtaining permission from the copyright owner is upon the account holder. Upon receiving proper notification, as defined by the Digital Millennium Copyright Act, of a potential infringing activity, we will where possible remove or block access to the material in question. Reports of repeated copyright infringements will lead to termination of computer/network services and/or other College/legal actions.

### **Access to computer accounts & networks / Non-commercial use only**

Ithaca College will make reasonable efforts to have its computer systems and networks available at all times. However, as part of regular maintenance and other planned and unplanned activities, systems & networks may be unavailable at any particular time. Ithaca College reserves the right to restrict or terminate access to its computer & network resources as necessary. Ithaca College computer systems and networks are for non-

commercial individual use related to the educational mission of the College by its faculty, staff and students, and for approved College business activities.

### **Abide by the regulations; don't break the law**

All users must abide by all college rules and policies, as well as local, state and federal laws. This includes, but is not limited to, other Information Technology Services policies; the Ithaca College Student Conduct Code and other College policies; local, state and federal regulations.

### **Privacy**

ITS follows industry practices and routinely monitors network traffic to ensure the proper functioning and equitable utilization of the college's computer resources, but by policy, does not routinely monitor the contents of user files, messages or network transmissions. However, given the nature of computers and electronic communications, we cannot guarantee the absolute privacy of your files and information. You must take reasonable precautions and understand that there is a risk that in some circumstances others can, either intentionally or unintentionally, gain access to files and messages.

Where it appears that the integrity, security or functionality of the College's computer or network resources are at risk or in instances of suspected abuse of College policies, codes, or local, state or federal laws, Ithaca College reserves the right to take whatever actions it deems necessary (including, but not limited to monitoring activity, scanning specific machines, and viewing files) to investigate and resolve the situation.

### **Restrictions**

The college may impose restrictions on the use of its computer and network systems and/or take additional actions in response to complaints presenting evidence of violations of this or other College policies, codes, or state or federal laws.

### **Reporting Violations**

If you believe that a violation of this policy has occurred, you should contact Information Technology Service's Computer Abuse Administrator at [computer\\_abuse@ithaca.edu](mailto:computer_abuse@ithaca.edu) or by calling 607-274-3030. In cases where you feel that an individual's health or safety appears to be in jeopardy you should immediately contact the Office of Campus Safety at 607-274-3333.

This policy will be updated periodically. Updates will always be posted to this page.

\*"Spamming" - the unauthorized sending of large volumes of unsolicited electronic mail or messages.