

# Restrictions on the Use of Napster

## TO: The NYU Community

In order to ensure NYU-NET availability is sufficient for NYU work, Information Technology Services (ITS) has been forced to take steps to restrict traffic related to an outside service called "Napster," which enables distribution of MP3 music files over the Internet.

In addition, in order to protect the security of NYU systems, we require that Napster software be removed from any NYU-owned machine on which it is installed. And we strongly recommend that it be removed from personally owned computers that are connected to NYU-NET.

The surging increase in Napster traffic on NYU-NET and with the Internet during recent weeks indicates that this service has become quite well known and popular at the University. However, it seems much less well understood that, because of the way the Napster service works, using it conflicts directly with the agreement an individual makes when:

(a) You register for an ITS account or any school or department account permitting network access (see "Responsibilities of All NYU Computer and Network Users," at [www.nyu.edu/its/policies/respon.html](http://www.nyu.edu/its/policies/respon.html));

(b) You connect your personal computer to NYU ResNet in the student residences (see "ResNet Accounts—Specific Policies and Information," at [www.nyu.edu/its/policies/resnet/](http://www.nyu.edu/its/policies/resnet/)).

NYU's "World Wide Web Policies and Procedures" also applies (see [www.nyu.edu/its/policies/webpolicy.html](http://www.nyu.edu/its/policies/webpolicy.html)).

Two main issues force ITS to highlight these policies and take steps to restrict use of Napster: network availability and computer security. In addition, individuals who have been using Napster need to be aware of some further considerations.

## 1) Network Availability

Traffic on NYU-NET increased dramatically in the past few weeks. Our analyses show that this increase is due largely to surging use of Napster, particularly on and from the ResNet leg of NYU-NET. Last Thursday night, for instance, before we put emergency restrictions

into place, NYU's Internet connection was operating at a dangerously high 98% of capacity. After the restrictions, traffic on the link dropped back to the more typical 60% of capacity.

It's not necessarily apparent when you're using Napster that you're generating much network traffic. Once you've downloaded your MP3 files, you might think you're done. But Napster in its default mode makes it possible for everyone else on the Internet to download files from your computer without your awareness or approval. Depending on the popularity of your collection, this feature can multiply many times the network traffic generated by your machine.

This Napster traffic surge has already interfered with the availability of the network for normal NYU work-related connections, which include University projects that require consistent network availability. NYU-NET resources exist to further the academic mission of the University. Though these resources are substantial, they are not infinite. Given the Napster surge, ITS has no choice but to restrict the Napster load on NYU-NET, so that the network remains available for NYU-related purposes. ITS had been planning to upgrade our link to the Internet as soon as the next generation of capacity comes online, later this year. That planning continues. In the meantime at least, these restrictions are essential.

## **2) Computer Security**

It's not readily apparent that, by running Napster, you can introduce serious security risks to your machine and the other files on it, as well as to other computers on the network. Napster disregards the security of individual computers in misleading ways that are unprecedented.

In the default configuration, when you download your first music file from Napster, you automatically also download Napster software that turns your computer into a file server. This software allows any other machine on the Internet to connect to your computer and download copies of your files without your knowledge or approval. Triggered by a request from the other machine, the Napster software on your computer then searches your hard drive and any mounted network drives for "music files to share."

Unprotected file sharing and file scanning create significant risks of compromise to your computer and your privacy, as well as to other computers on NYU-NET. There is no way to tell what malicious functions may be performed by the software you automatically download with the music or what modifications may have been made to the music files themselves. This security issue is further complicated by Napster's decision to release the source code for the software it downloads onto your machine. The resulting proliferation of authors and versions makes your machine even more vulnerable to unexpected intrusions.

## **Further Considerations for Those Using Napster**

Because Napster can automatically turn your computer into a server, it increases the possibility of automatically turning you into a distributor of music files without the creator's permission. Distribution is a step more serious than simply copying these files and can be a violation of U.S. copyright laws. In this regard, it's worth noting that Napster keeps a database of the IP addresses of all the individual computers that use Napster software to distribute MP3 files.

Thanks for your cooperation in addressing what so quickly became a serious threat to both network availability and computer security at NYU. We will, of course, continue to monitor the situation and may take further steps as they become necessary.

Marilyn McMillan  
Chief Information Technology Officer  
New York University

For more information see [http://www.nyu.edu/its/policies/napster\\_faq.html](http://www.nyu.edu/its/policies/napster_faq.html) and for current network status see <http://www.nyu.edu/its/status/>.

All contents copyright  
© New York University.  
All rights reserved.  
Page last revised: **June 1998**  
Page last reviewed: August 22, 2006