# HARVARD UNIVERSITY RESNET
Appropriate Use Policy
December 20, 2002

## Use of Computers and Networks

Individuals who are provided access to University computer facilities and to the campus–wide communication network assume responsibility for their appropriate use. The University expects individuals to be careful, honest, responsible, and civil in the use of computers and networks. Those who use wide–area networks (such as the Internet) to communicate with others or to connect to computers at other institutions are expected to abide by the rules for the remote systems and networks as well as those for Harvard's systems. Be advised that, in addition to being a violation of Harvard University rules, certain computer misconduct is prohibited under Massachusetts General Laws, c.266 subsection 33 (a) and 12 (f) and is, therefore, subject to criminal penalties. Such misconduct includes knowingly gaining unauthorized access to a computer system or data base, falsely obtaining electronic services or data without payment of required charges, and destroying of electronically processed, stored, or in–transit data.

Individuals are expected to abide by these rules and policies and to consult an official of Harvard University prior to any activity that would appear to threaten the security or performance of University computers and networks.

## Use of Facilities

Individuals may not attempt to damage or to degrade the performance of Harvard's computers and networks and should not disrupt the work of other users. Individuals may not attempt to circumvent security systems or to exploit or probe for security holes in any Harvard network or system, nor may individuals attempt any such activity against other systems accessed through Harvard's facilities.

Execution or compilation of programs designed to breach system security is prohibited unless authorized in advanced. Moreover, the possession or collection of others passwords, personal identification numbers (PINs), private digital certificates, or other secure identification information is prohibited.

Use of Harvard's computers and networks for business–related purposes without authorization is prohibited. Unauthorized use of the Harvard University Network, computer systems, or facilities is prohibited. Individuals should not attempt to exploit, test, or probe for suspected security holes on Harvard University computers or networks, but instead should report them to Harvard University’s Network Operation Center. Likewise, users should not disseminate to others any information that serves to circumvent or degrade system or network security or integrity.

Physical theft, rearrangement, or damage to any University computer or network equipment, facilities, or property is strictly prohibited, and will be reported to the police. This includes all public computer labs, network hubs, wiring, and links.

Harvard University must ensure that academic work takes precedence at all times over other computing activities in its facilities. In situations of high user demand that may strain available computer resources, Harvard University reserves the right to restrict (e.g., to specific times of day) or prohibit computer entertainment activities such as game playing.

Individuals must abide by all official posted rules and official communications from Harvard University regarding use of facilities and resources.

## Use of the RESNET Network

Users with personal computers on the RESNET Network are expected to take reasonable precautions to ensure the security of their systems. Individuals may be held responsible for misuse by others that occurs on their systems.

Attempts to monitor, analyze, or tamper with network data packets that are not explicitly addressed to your computer are prohibited.

Using a network address other than the one assigned by Harvard University is prohibited.

Users are not permitted to register external domain names (i.e., any domain outside of harvard.edu) that reference systems on the Harvard University Network without authorization.

Users may not advertise routing information on the Harvard University Network or act as gateways to external or private networks.

It is prohibited to connect any secondary physical network, including bridges, routers, or wireless access points, to the Harvard University Network without authorization.

Providing services or running applications that consume excessive bandwidth or impede others' use of the Harvard University Network is prohibited without authorization.

## Privacy of Information

Information stored on a computer system or sent electronically over a network is the property of the individual who created it. Examination, collection, or dissemination of that information without authorization from the owner is a violation of the owner's rights to control his or her own property. Systems administrators, however, may gain access to users data or programs when it is necessary to maintain or prevent damage to systems or to ensure compliance with other University rules.

Computer systems and networks provide mechanisms for the protection of private information from examination. These mechanisms are necessarily imperfect and any attempt to circumvent them or to gain unauthorized access to private information (including both stored computer files and messages transmitted over a network) will be treated as a violation of privacy.

In general, information that the owner would reasonably regard as private must be treated as private by other users. Examples include the contents of electronic mail boxes, the private file storage areas of individual users, and information stored in other areas that are not public. That measures have not been taken to protect such information does not make it permissible for others to inspect it.

On shared and networked computer systems certain information about users and their activities is visible to others. Users are cautioned that certain accounting and directory information (for example, user names and electronic mail addresses), certain records of file names and executed commands, and information stored in public areas, are not private. Nonetheless, such unsecured information about other users must not be manipulated in ways that they might reasonably find intrusive; for example, eavesdropping by computer and systematic monitoring of the behavior of others are likely to be considered invasions of privacy. The compilation or redistribution of information from University directories (printed or electronic) to third parties, especially those outside the University, is forbidden.

## Electronic Communication

Harvard University neither sanctions nor censors individual expression of opinion on its systems. The same standards of behavior, however, are expected in the use of electronic mail as in the use of telephones and written and oral communication. Therefore electronic mail, like telephone messages, must be neither obscene nor harassing.  Similarly, messages must not misrepresent the identity of the sender and should not be sent as chain letters or broadcast indiscriminately to large numbers of individuals. This prohibition includes unauthorized mass electronic mailings. For example, email on a given topic that is sent to large numbers of recipients should in general be directed only to those who have indicated a willingness to receive such email.

## Intellectual Property

Computer programs written as part of one's academic work should be regarded as literary creations and subject to the same standards of misrepresentation of copied work. In addition, attempts to duplicate, use, or distribute software or other data without authorization by the owner is prohibited.

Under federal copyright law, no copyrighted work may be copied, published, disseminated, displayed, performed, or played without permission of the copyright holder. Harvard may terminate the network access of users who are found to have repeatedly infringed the copyrights of others.

## Cases of Misconduct

Whenever a case of computer misconduct is suspected or reported,  Harvard University reserves the right to deny system or network access on a temporary basis to anyone who violates these rules. This includes the ability to terminate processes or connections that threaten system or network security, performance, or integrity.

## Waiver

Users recognize that systems and networks are imperfect and waive any responsibility for lost work or time that may arise from their use. The staff of Harvard University cannot compensate users for degradation or loss of personal data, software, or hardware as a result of their use of University–owned systems, software, or networks, or as a result of assistance they may seek from Harvard University staff.