Interim Policy on
Acceptable Use of Information Resources

General Principles

The University's computer systems and networks are shared resources used by many individuals to carry out the University's mission of teaching, research, and service. Use of these resources must be ethical, reflect academic honesty, respect the rights of other users, demonstrate respect for intellectual property and ownership of data, respect system security mechanisms, and promote an environment free from intimidation and harassment.

By using University computer systems and networks, users agree to abide by and comply with the applicable policies, procedures, and laws. All examples given below are illustrative. Application of this policy is not limited to the examples presented.

Users of computer systems and networks have the responsibility to:

- comply with all University policies, procedures, relevant employment contracts, and local, state, and federal laws.
- use computer systems and networks for authorized administrative, academic, research, or clinical purposes or other University business.
- protect user-IDs and computer systems and networks from unauthorized use. Users are responsible for all activities that originate from their accounts or systems that they perform or have expressly authorized in accordance with the Policy on Password Sharing.
- access only information that is their own, that is publicly available, or that they have been authorized to access.
- comply with all copyright laws, licensing terms, patent laws, trademarks, and trade secrets.
- use information systems in a way that does not infringe on the ability of other users to reasonably access computer systems and networks.

The following are examples of uses that are unacceptable:

- use another individual's user ID or password without the proper authorization as described above.
- use computer programs to decode passwords or access system control information without proper authorization.
- attempt to circumvent or subvert system or network security without proper authorization.
- engage in any activity that might be harmful to the systems or to any information on the systems, such as creating or propagating viruses, disrupting services, damaging files, making unauthorized modifications to University data, or unauthorized sharing of University data.
- use University systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
- harass or intimidate another person, such as repeatedly sending unwanted mail or sending threatening mail.
- monopolize information systems without proper authorization. Examples of monopolizing systems include: removing shared manuals from a laboratory, uploading and downloading files of sufficient size or quantity to degrade network performance for other users, sending out or forwarding chain letters, and sending large unauthorized mass mailings.
- attempt to gain access to information or services without proper authorization.
- engage in any other activity that does not comply with the General Principles presented above, University policies and procedures, or applicable law.