UNIVERSITY OF MAINE SYSTEM

SUBJECT: INFORMATION TECHNOLOGY ACCEPTABLE USE

The University provides information technology resources (dial-up, networks, servers, laptops, telephony, email etc.) for education, research and public service. This policy applies to all users including faculty, staff, students and guests.

Availability

The University extends all users the privilege to use these resources in a responsible, ethical and legal manner.

- All users should respect the constraint of finite system bandwidth supporting data, video and voice and minimize any optional transmittal of large amounts of data during peak use periods.
- Staff , Faculty and Guest personal use is permitted when use does not interfere with the University's mission.
- Neither the name of the University, its campuses, an email address nor a user's position may be used to imply University support for any non-university advocacy issue nor may the resources be used for personal financial gain.
- Users who abuse their privilege may lose access to the information technology resources.

Privacy

The University respects a users' right to privacy but cannot assure privacy; therefore, users should expect only a limited level of privacy.

- Data on a shared resource such as on a PC or in shared storage may be available to multiple users.
- Some data stored on University resources may be considered public records subject to disclosure to third parties.
- The information technology resources must be available to support the University's mission. Staff may need to inspect the resources to maintain or improve the function, if there is a suspicion of misconduct or if there may be a violation of Federal, State, local law or evidence of violation of University Policy.

Security

Users should assume that unencrypted data is insecure.

- Unencrypted data stored on the network or on an individual PC may be read or compromised.
- Unencrypted email and data transfer is subject to unauthorized interception, alteration and counterfeiting.

Implementation and Enforcement

- UMS-ITS (University of Maine System Information Technology Services) is responsible for the security and privacy of the shared systems under UMS-ITS' control.
- Each campus is responsible for security and privacy of the systems they manage and for violation management.
- Individual campuses may enact additional Acceptable Use Standards that will include these minimum standards.

The Campus Information Technology Director will notify the University of Maine System Chief Information Officer of any significant violation of acceptable use including any violation that results in loss of access privileges or which may have implications beyond a single campus or may involve private, financial or medical information.

Examples of acceptable and unacceptable use follow.

UNIVERSITY OF MAINE SYSTEM

SUBJECT: INFORMATION TECHNOLOGY ACCEPTABLE USE

USE EXAMPLES

UNIVERSITY'S NAME OR USER'S POSITION

Acceptable:	• Participation in a professional list serve which may identify the user with the University by name, position or email address.
Unacceptable:	• Hosting a list-serve, web site, or information exchange that is not related to the mission of the University. For example, an information exchange in association with advocacy-issue oriented activities. • While running for political office, using a University email account to send email about your candidacy to people who live in your district promoting you as a candidate

SPAMMING

Acceptable:	• The incidental solicitation of contributions or purchases from a select group of coworkers for a charitable cause (i.e. walk-a-thons, March of Dimes, Girl Scout Cookies)
Unacceptable:	• Sending unsolicited, unwanted, irrelevant, or inappropriate messages in mass quantities

BURDENING THE RESOURCES

Acceptable:	• Storing and sending email messages, files, pictures using modest amounts of shared network file storage and transmission capacity consistent with the mission of the University • Web based surveillance systems
Unacceptable:	• Spamming the System • Using a video camera to continuously display what is happening in your office, department or work area, and serving the video on the web. • Maintaining a large file of images in shared network folders
Discouraged:	• Use of wallpaper, signature graphics or imbedded images in routine email messages • Sending large attachments when links are available

PERSONAL USE

Acceptable:	• When employees are "off the clock" or in "downtime" sending brief personal email, accessing the Internet, sending or responding to brief instant messaging, playing games, using programs on a University PC or using modest amounts of file storage
Unacceptable:	• Operating a business using a University PC or other IT resource • User operation of sniffing or other programs normally associated with network traffic identification, scanning or management. (Exceptions may be made for class work in connection with network security management)

COMPLIANCE WITH LAWS

Acceptable:	• Storing legitimately obtained audio files for use in language instruction.
Unacceptable:	• Participating in a chat room in violation of any law such as to solicit sex from a minor • Copyright infringement, typically of music or text

APPROVED

Chief Financial Officer and Treasurer