



*Updated as of June 29, 2011*

Framingham State University's computing and electronic communication resources are the property of the University and are made available to authorized users for teaching, learning, research, administration, public service and other approved purposes. Protecting and preserving the University's computing and electronic resources is a cooperative effort that requires each member of the University community to act responsibly and guard against abuses. This policy is established in an effort to help users understand what is required of them in exchange for the privilege of access to these resources. It sets guidelines regarding the issues of privacy and respect for property, ownership of data, system security, and responsible use in ways that are ethical and that demonstrate academic integrity and respect for others who share these shared resources.

This policy applies to all users of University computing and communications resources, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to computing resources provided or operated by individual units of the University or to uses within specific departments.

The University provides authorization to use University computing and electronic communications resources with the creation of a user ID and password to individuals who agree to the terms and conditions of the Acceptable Use Policy (AUP). Third party service providers and contractors are expected to inform their own staff of the University's AUP. Individuals who refuse to accept and follow the AUP will not be granted authorized access.

#### **ACCEPTABLE USE**

Acceptable use begins with respecting ownership rights of other users and organizations including intellectual property, data, and physical resources. And it extends to include ensuring system security, integrity of communications, and compliance with all relevant policies, regulations and contractual obligations.

Use of University computing and electronic communication resources requires each user to adhere to the following standards of acceptable use:

- Observe all federal and state laws, as well as policies of Framingham State University, with respect to use of University computing and electronic communication resources.
- Respect the privacy and personal rights of others by ensuring that use of University computing and electronic communication resources does not constitute invasion of privacy, harassment, defamation, threats, intimidation, or discrimination based on race, sex, national origin, disability, age, religion, or sexual orientation.
- Preserve the performance, integrity, and security of University computing and electronic communication resources. Ensure that use of those resources does not circumvent system security and does not achieve or aid others to achieve unauthorized access.
- Protect the intellectual property rights of others by ensuring that use of University computing and electronic communication resources does not violate and copyright, trademark, file protections or other security boundaries.

#### **Academic Integrity**

Just as in any other aspect of a student's academic work, the University expects that students will use computing and electronic communication resources in ways that are honest and ethical. Actions that constitute academic dishonesty include:

- Turning in someone else's work as your own.
- Allowing someone to represent your work as his or her own.
- Several people working on one paper and submitting it individually, as if each had done the paper alone.
- Using another's work without proper acknowledgment.

## **Respectful Exchange of Ideas and Information**

Computer systems and networks allow for a free exchange of ideas and information. This exchange serves to enhance learning, teaching, critical thinking and research. While the constitutional right of free speech applies to communication in all forms, civil and respectful discourse is strongly encouraged. University policy and local, state and federal law do prohibit some forms of communication, including:

- Harassment, invasion of privacy, threats, defamation, intimidation, obscenity, and anonymous or repeated messages designed to annoy, abuse or torment.
- Discrimination based on race, sex, national origin, disability, age, religion, sexual orientation or other protected status.
- Advocacy directed to incite, facilitate or produce lawless action.

## **Responsible Use**

Computing and electronic communication resources are made available to all Students, Faculty and Staff. Because there are so many individuals who utilize this shared resource, respect for the rights and needs of others is central to this policy. To ensure access and service for all, users must refrain from any of the following specifically unacceptable uses of computing and electronic communication resources:

- Any action that jeopardizes the availability or integrity of any University computing, communication or information or intentional use of these resources to disrupt University operations and/or academic programs.
- Chain letters and mailings to large numbers of people that contain unwanted solicitations or information. These mailings are often referred to as "spam".
- Use in a manner that interferes with the work of other Students, Faculty or Staff.
- Use for profit activities (advertising, sales, consulting for pay, and so on) or use by for-profit institutions unless otherwise authorized.
- Use for private or personal business in violation of University policies.
- Anonymous mailings or mailings which impersonate another individual.
- Allowing anyone else to use your login credentials.

## **Prohibited Use**

University computing and electronic communication resources must not be used in a manner that could compromise security, infringe upon property rights or violate privacy. The following restrictions are imposed to protect everyone. Users are prohibited from:

- Using computer or network services in a way that violates copyrights, patent protections or license agreements.
- Attempting to bypass University information security.
- Gaining unauthorized access to information that is private or protected, or attempting to do so.
- Running programs that attempt to identify passwords or codes and installing network monitoring tools by anyone other than authorized personnel.
- Interrupting programs that protect data or secure systems, or attempting to do so.
- Monitoring or tampering with another person's e-mail.
- Tapping telephone or computing network communications in violation of federal or state law.
- Reading, copying, changing or deleting another person's work.
- Attempting to make unauthorized changes to information stored on University owned systems.
- Attempting to make unauthorized copies of information stored on University systems.
- Using another person's login credentials, or allowing others to use yours.
- Attempting to gain network privileges to which you are not entitled.
- Impersonating another, real or not, individual, machine or organization.

## **PERSONAL RESPONSIBILITY**

Each individual who is provided access to computing and electronic communication resources made available by the University, must understand that he or she is accountable for the policies set forth in this documentation. In addition, each user assumes responsibility for:

- Protection of his or her password.
- Reporting any breach of system security.
- Reporting unauthorized use of his or her account.
- Changing his or her password on a regular basis.
- Frequently making back-up copies of work to ensure against loss.

## **COMPUTER VIRUSES**

Users should exercise reasonable precautions in order to prevent the introduction of malicious software into the campus computing network. Virus scanning software should be used to check any software downloaded from the Internet or obtained from any questionable source. In addition, executable files (program files that end in ".exe") should not be stored on or run from network drives. It is also recommended that portable media be scanned periodically to ensure against infection.

## **E-MAIL**

When using e-mail, there are several points users should consider. First, because e-mail addresses identify the organization that sent the message ([username@framingham.edu](mailto:username@framingham.edu)) users should consider e-mail messages to be the equivalent of letters sent on official letterhead. For the same reason, users should ensure that all e-mails are written in a professional and courteous tone. Finally, although many users regard e-mail as being like a telephone, in offering a quick informal way to communicate, users should remember that e-mails can be stored, copied, printed or forwarded by recipients. As such, users should not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum.

## **NO EXPECTATION OF PRIVACY**

All University computing and electronic communication resources are the property of the University and the Commonwealth of Massachusetts and shall be used in conformance with this policy with no expectation of privacy. The University retains the right to inspect any user's computer, any data contained in it, and any data sent or received by that computer. The University reserves the right to monitor and record the usage of all computing resources as necessary to evaluate and maintain systems and acceptable use; and may monitor, record and legally disclose usage by individuals, including the disclosure of individual files.

## **ENFORCEMENT**

All members of the University community are bound by federal and state laws relating to civil rights, harassment, copyright, security and other statutes relating to electronic media. This policy does not preclude enforcement under the laws and regulation of the United States of America or the Commonwealth of Massachusetts.

Violation of this policy may subject a user to disciplinary action under the appropriate University procedures. The University may take such action as necessary, in its discretion, to address any violation(s) under this policy including referral to appropriate authorities.

## **DISCLAIMER**

The University makes no warranties of any kind, whether express or implied, for the service it is providing. The University will not be responsible for any damages a user may suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions cause by Framingham State University negligence or by the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The University specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information they obtain and consider how valid that information may be.

The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic resources and communication are warned that they may come across or be recipients of material they find offensive.

The University reserves the right to change this policy at any time without notifying individuals affected by the policy.