PN 6.001

# FROSTBURG STATE UNIVERSITY

# ACCEPTABLE USE OF UNIVERSITY COMPUTING RESOURCES POLICY

**(Approved as of October 15, 2015)**

## I. POLICY

A. The personal obligations of each member of the University community include using computing resources responsibly, ethically and in a manner within the law and the rights of others. The University depends upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

B. Freedom of expression and an open environment to pursue scholarly inquiry and for sharing of information are encouraged, supported, and protected at Frostburg State University. Censorship is not compatible with the tradition and goals of the University. While some computing resources are dedicated to specific research, teaching or administrative tasks that limit their use, freedom of expression must, in general, be protected. The University does not limit access to information because of its content when it meets the standard of legality.

## II. PURPOSE

A. The purpose of this policy is to assist users in using the University computing and network facilities responsibly and safely, and to assure that the system is used responsibly, legally, and with respect for the privacy of others. The University is concerned chiefly with identifying and responding to violations by members of the University community that directly affect the University and that are defined by the Student Code of Conduct, the Faculty Handbook, Personnel Policies, and/or other applicable policies and procedures. Should any violations of this policy originate in the University's network, extend beyond the University community, or be reported to the University by outside authorities, the University reserves the right to take appropriate actions (as described herein) against the violator.

## III. SCOPE

A. Frostburg State University (“FSU” or the “University”) is a member of the National Information Infrastructure through its campus network. As a member of the University community, users of the network are responsible for protecting the integrity of the system. A "user" or “authorized user” is any individual who uses, logs in, attempts to use, or

attempts to log in to the FSU computer system, whether by direct connection or through one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software or both. In accessing the FSU network, all users shall adhere to, and network connecting devices shall conform to, the policies set forth in this document.

B. Use of the campus network and all components of the network is not a right, but rather a privilege granted by the University. The campus network and many of the components that make up, or are attached to the network, are the property of the State of Maryland. When using the network, users are subject to the laws of the State of Maryland related to the use of state property. When accessing the systems of other institutions, users are subject to the rules of use for that particular institution as well as those for FSU.

C. By establishing this policy for responsible computing, the University is not undertaking the responsibility to screen or control the content of messages or other electronic data transmitted through the University system, although it may choose to do so as permitted by law and University policy. The University specifically denies any responsibility for the accuracy or quality of information obtained through its computing and electronic communications facilities and services. Further, the University makes no warranties of any kind, whether expressed or implied, for the service it is providing. The University is not responsible for any damages suffered through the use of its computing and electronic communications facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, or service interruptions caused by the University's negligence or by user error or omissions. Use of any information obtained via the Internet is done so at the risk of the user.

## IV. PROCEDURES

A. Campus Network Responsibility

Each individual user is responsible for understanding and complying with the guidelines contained in this policy. All authorized users are responsible for the security of their passwords and accounts. In addition, users assume personal responsibility for the content of their accounts, their electronic transmissions, and their overall activities while using the campus network and attached devices, regardless of the resource used to access or store the data, whether an institutional system, a privately owned resource, or a third-party resource, including electronic communication that would be deemed a violation of University sexual harassment and/or other harassment or discrimination policies, federal or state laws, or other regulations.

B. Intended Use of the Campus Network

i. The University's computer system is available for authorized users only and only within the scope of their authorization. Unauthorized access to and use of University computers is prohibited.

ii. Internet access and e-mail provided by the University are intended for educational use, instruction, research and the facilitation of communication, collaboration, and other University related purposes.

iii. All use of the network, including e-mail and the internet, may be monitored. The University has the right to inspect, without notice to the user, any work created on or information transmitted over the network, including all e-mail messages that are sent or received on the network, accessed internet sites, and information downloaded from or transferred via the internet. By accessing and using University computers and networks, you are consenting to such monitoring and information retrieval for law enforcement and other purposes.

iv. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit. It is the policy of the University that University resources, including computer equipment, should not be used by University faculty or employees to access, download, print or store any information infrastructure files or services having sexually explicit content, unless for valid academic or business purposes. Unauthorized use or misuse of the network may result in disciplinary action.

C. Passwords

Computer account "userid" identifies the user to the Internet user community. Anyone who knows a user's password can use that account. If he or she does anything that affects the system, it will be traced back to the userid. If a user's computer account is used in an inappropriate manner, the user can be held responsible for the consequences.

D. Use of Copyrighted Material

i. Many software programs, images, sounds, text, and related materials such as documentation are protected by copyright and other laws and by licenses and other contractual agreements. Users must abide by these restrictions. To do otherwise is a crime or a violation of legal rights for which users may be personally liable.

ii. Such restrictions include prohibitions against copying data, images, sounds, or programs, the resale of this material or the use of this material for non-educational purposes or for financial gain, and public disclosure of information about programs (e.g., source code) without the owner's authorization.

iii. Users must abide by all software licenses, FSU and USM copyright and intellectual property policies, and applicable federal and state laws.

E. Privacy Of Users

i. Federal law protects the privacy of users of wire and electronic communications. Users shall not permit their use of the campus network and other computing

facilities to violate the privacy of other users, even if unintentionally. Specifically, unless otherwise allowed by law or University policies and procedures:

ii. Users shall not access the files or directories of another user without clear authorization from that user. Typically, this authorization is signaled by the other user's setting file access permissions to allow public or group reading of the files.

iii. Users shall not intercept or otherwise monitor any network communications not explicitly meant for the user. These include e-mail and user-to-user dialog, as well as a user's password input.

iv. Users shall not use the system to store personal information about individuals that they would not normally disseminate freely about themselves.

v. Users shall not create programs that secretly collect information about other network users without their prior consent.

F. Misrepresentation

Misrepresentation of a user as another individual is not allowed on the FSU campus network or in any electronic communication with other parties. In addition, the campus network may not be used to express a personal opinion or belief that may be interpreted as an expression of the University's viewpoint.

G. Use of E-Mail

i. The University considers an E-mail communications as a business correspondence; therefore, you should use and respond to e-mail in a manner consistent with other business communications. The purpose of the campus network is to support research, education, service, and administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of your campus network must be consistent with this purpose. E-mail communications made or received by University employees using University facilities are presumed to be made in the course of University employment and are subject to rules, regulations and laws pertaining to University records and policies. Occasional and incidental social communications using e-mail are not prohibited; however, such messages should be limited and must not interfere with an employee's job function. The campus network is never to be used for commercial purposes or solicitation without authorization from proper University officials.

ii. Guidelines on the use of E-mail are not based on etiquette alone. As provided in Paragraph 11 below, any e-mail generated by University employees on the on-campus network is presumed to be University property and therefore may be subject to disclosure. E-mail may be and has been used as a source to support litigation claims. Furthermore, E-mail sent with the intent of disrupting communication or other system services is not allowed. The proliferation of electronic chain letters is abusive to the mail system and the network. Chain

letters waste valuable computing resources. You may lose your network privileges by creating or forwarding chain letters.

iii. As with certain other forms of communication, security of e-mail transmissions cannot be absolutely guaranteed. Users should consider whether an alternative form of communication should be used for particularly sensitive information.

H. Unlawful Activities and Violations of University Policy

i. Knowingly using the campus network or computing resources for illegal or criminal purposes or in violation of University policy may result in suspension of network privileges and components attached to the network, as well as other disciplinary and/or legal action. Illegal or criminal use may include obscenity, child pornography, threats, harassment, discrimination, copyright infringement, University trademark infringement, defamation, theft, identity theft and unauthorized access.

ii. Discrimination and/or harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation, or age may be a violation of law and/or University policy. Sexual harassment means any unwelcome sexual advances, unwelcome requests for sexual favors or other unwelcome verbal, physical, or electronic conduct of a sexual nature that has the purpose or effect of unreasonably interfering with an individual's academic or work performance, that is, it is sufficiently severe, persistent, or pervasive to enough to create an intimidating, hostile, humiliating, demeaning or sexually offensive working or learning environment. Sending unsolicited or unwanted E-mail or messages that constitutes sexual harassment or discrimination may be subject to disciplinary or legal action by the University.

I. Computer Viruses and Malware

The deliberate introduction of a computer virus or other malware into an FSU computer or computing system is against both federal and state law as well as a violation of FSU policy. Attempts to introduce such viruses may result in suspension of computing privileges as well as other legal and/or University action.

J. Masking Activity

The deliberate masking or hiding of activity on the network is prohibited. Using a computer account for which authorization has not been granted, using the campus network to gain unauthorized access to any computer system, attempting to circumvent data protection schemes or uncover security loopholes, or masking the identity of an account or machine may result in suspension of computing privileges as well as other legal and/or University action. This includes unauthorized connections from off-campus or other network segments as outlined in the FSU Virtual Private Network Policy.

K. Limited Right to Privacy

i. To the extent possible in the electronic environment and a public setting, a user's privacy will be preserved. Consistent with applicable law and University policies

and procedures, including those pertaining to University records, all users should treat electronically stored information in individual files as confidential and private. Contents should be examined or disclosed only when authorized by the owner, approved by an appropriate University official, or required by law. Attempts by unauthorized individuals to read or access another person's e-mail or other protected files will be treated with the utmost seriousness. However, the University reserves the right to monitor its computing resources to protect the integrity of its computing system workstations, and lab facilities.

ii. University system administrators may conduct periodic security checks of the campus network and attached components, including password checks, to determine if security violations or other violations of this policy have occurred or are occurring. Any user with a "bad password" will be notified via e-mail. Passwords must be changed in a timely manner or the user will be "locked out" of the account and must contact Academic Computing to rectify the problem.

iii. Privacy of records stored in the electronic environment is subject to applicable federal and state law, and the needs of the University to meet its administrative, business and legal obligations. FSU is an agency of the State of Maryland and therefore subject to the Maryland Public Information Act (Maryland Annotated Code, State Government Article, 10-611 et seq.). Stored electronic information and e-mail are generally considered public records. Privacy of such records, unless subject to a specific privilege, may be subject to review and/or release under federal law and the Maryland Public Information Act. Electronic information, including e-mail messages, when relevant, are subject to production through discovery in civil litigation.

iv. Administrative files of the University are generated as part of the process of managing the University. Files that employees create or maintain as well as e-mail can be reviewed by supervisors within this administrative context. Generally, faculty research files and files relating to scholarly endeavors will not be subject to such a review.

v. In the normal course of system administration, system administrators may have to examine activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware. In this case, the user should be notified as soon as practical. Computer systems and stored data are subject, by authorized personnel, to review for audit purposes or when a violation of University policy or law is suspected.

L. Compliance with Law

All users of University computing resources must comply with all state, federal, and other applicable law; all generally applicable University rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; the University's Code of

Student Conduct; the University's Sexual Misconduct, Relationship Violence and Stalking Policy; the University's personnel policies; and all applicable software licenses. Users who engage in communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

M. Disciplinary Actions for Abuse of Privileges

i. Violation of the provisions of this policy constitutes unacceptable use of computing resources and may violate other University policies and/or state and federal law. Known or suspected violations should be reported to the Office of Information Technology.

ii. Users who violate this policy may be denied access to University computing resources and may be subject to other penalties and disciplinary action, both within and outside of the University. The University may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of University or other computing resources or to protect the University from liability. Violations will be handled through University disciplinary procedures applicable to the relevant user. Policy violations by students will be handled in accordance with the Code of Student Conduct. Policy violations by University employees, including faculty, will be handled in accordance with the USM and University Personnel Policies, the Faculty Handbook and other applicable administrative policies and procedures. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

## IV. RESPONSIBLE DEPARTMENT

A. The University's Offices of Information Technology (x7090) is responsible for implementing this policy and may be contacted regarding questions about the policy or to report violations of the policy.