

University Policy 5.1: Responsible Use of University Computing and Electronic Communications Resources

I. Purpose

The computing and electronic communication resources that Alabama A&M University provides for faculty, staff, and students are essential to carrying out the University's mission.

The rights of academic freedom and freedom of expression apply to the use of university computing resources. So too, however, do the responsibilities and limitations associated with those rights. The university supports a campus and computing environment open to the free expression of ideas, including unpopular points of view. However, the use of university computing resources, like the use of other university-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible.

III. Standards of Responsible Use

Users of university computing resources must comply with federal and state laws, university rules, policies and procedures, and the terms of applicable contracts including software licenses while using university computing resources. Examples of applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Alabama

a particular use of university computing resources should contact the Office of the General Counsel for more information.

Use of University computing and electronic communication resources is conditioned upon the obligation of each user to adhere to the following standards of responsible use:

1. Each User is required to behave responsibly with respect to the University Network and other Users at all times.
2. Each User is required to respect the integrity and the security of the University Network.
3. Each User is required to behave in a manner consistent with University's mission and comply with all applicable laws, regulations, and University policies and procedures.
4. Each User is required to be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to use the University Network and show restraint in the consumption of shared resources.
5. Each User is required to respect the rights and property of others, including privacy, confidentiality and intellectual property.
6. Each User is required to cooperate with the University to investigate potential unauthorized and/or illegal use of the University Network.
7. Each User is required to respect the security and integrity of university computer systems and data.
8. Privately-owned computer systems or those owned by collaborative research projects, when attached to, or connected via, the campus data network and/or other campus resources are subject to the same responsibilities and regulations as pertain to University-

- x Publishable research;
- x Personal computing to improve computing literacy, or to learn new computer hardware and software;
- x Use of public computers for review of generally available individual or campus information;
- x Use of computers provided by the university to faculty and staff in support of their work;
- x Approved use of the university's information and administrative systems; and
- x Use of Internet resources to promote collegial interaction and research.

VI. Violation of Policy

Violations of responsible use of University computing and electronic communication resources include, but are not limited to the following:

1. **Prohibited Behavior:** Storing, transmitting or printing any of the following types of Electronic Communications on the Computer System is prohibited: material that infringes upon the rights of another person; material that is obscene; material that consists of any advertisements for commercial enterprises; material or behaviors that violate the Alabama A&M University Code of Student Conduct or other University Policies or Procedures; or material that may injure someone else and/or lead to a lawsuit or criminal charges.
2. **Identity Fraud:** Users may not attempt to disguise their identity, the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may likewise not misuse or appropriate the University's name, network names, or network address spaces.
3. **Privacy Infringement:** Users may not attempt to intercept, monitor, forge, alter or destroy another User's communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of such other User.
4. **Hacking or Spamming:** Users may not use the University Network in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any computer, the network, or any other University resource; or (b) interferes with the University's operations.

electronic communication distributed or sent within the University Network or to other networks while using the University Network.

7. **Network Security Infringement:** Users may not attempt to bypass network security mechanisms, including those present on the University Network, without the prior express permission of the owner of that system. The unauthorized network scanning (e.g., vulnerabilities, port mapping, etc.) of the University Network is also prohibited. For permission to perform network scans, user must receive prior approval by calling 372-HELP (4357) and submitting a ticket to the Information Security Office.
8. **Unauthorized use of data:** Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express

resolve problems. If problem traffic patterns suggest that system or network security, integrity, or performance has been compromised, network systems staff will investigate and protective restrictions may be applied until the condition has been rectified. Access to other transmissions sent or received through the University Network may occur in the following circumstances:

1. In accordance with generally accepted, network-administration practices; 1.elib7.-6(i)8a(o)-2(gs)-1(;PI)-1(;) 1.

IX. Compliance

Failure to comply with this Policy and/or regulations promulgated hereunder will be deemed a violation of University Policy and subject to disciplinary action in accordance with the disciplinary guidelines as outlined in the Faculty or Staff Handbook, whichever one is applicable to the individual.

Revision History

- x Initially approved: December 2011 (Procedure)
- x Policy Approved December 2012 (Board Approval)

Authority: President

Responsible Office: Information Technology Services