Policy Name: Responsible Use of Computing Resources
Policy ID Number: 03-05-001
Version Effective Date: December 8, 2009
Last Reviewed on:
Applies To:

Use another person's User ID, password, files system or data.
Use computer programs to decode passwords or access control information.
Attempt to circumvent or subvert system security measures.
Attempt to modify or destroy University computing or communications equipment.
Remove any University computing or communications equipment without proper authorization.
Engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
Use University systems for partisan political purposes, such as using electronic mail to circulate advertising for political candidates.
Download, copy or use material from the Internet in violation of copyright laws.
Use mail or messaging services to harass, intimidate, or otherwise annoy another person, for example, by broadcasting unsolicited messages or sending unwanted mail.
Use social networking or sharing web resources to harass, intimidate, or otherwise annoy another person, for example, by posting slanderous comments about a member of the university on Facebook, Twitter, etc.
Use the University's systems for personal gain, for example, by selling access to your User ID or by performing work for profit in a manner not authorized by the University.
Use the University' systems for commercial purposes unrelated to academic and/or University related work.
Make or use illegal copies of copyrighted software, video, or music, store such copies on University systems, or transmit them over University networks.
Use the University's systems for any illegal activity.
Engage in any other activity that does not comply with General Principles presented above.

Potential Consequences for Violations

The University considers any violation of this appropriate use policy, principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on University systems allegedly related to inappropriate use. Violators are subject to disciplinary action including loss of all University computing privileges and possible criminal charges including civil damages. Offenders also may be prosecuted under various state & federal laws including (but not limited to) the Privacy Protection Act of 1974, The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication of 1989, Interstate Transportation of Stolen Property, and the Federal Electronic Communications Privacy Act. Access to the texts of these laws is available through the Reference Department of the Library. Violators may also cause the University to be liable to civil or criminal penalties.

As deemed necessary or appropriate by the Policy Coordinator but at a minimum, at least every 5 years from the date of last review.