Acceptable Use Policy

Objective

The purpose of the Acceptable Use Policy is to establish acceptable and appropriate use of University Information and University Information Resources, which exist to support the educational mission, business and other administrative requirements of Suffolk University.

Applicability

The Acceptable Use Policy applies to all University students, faculty or staff members, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any third party service provider providing services to the University who create, use or otherwise access or interact with any University Information or University Information Resource ("University Users").

Definitions

University Information: any information in any form whether electronic, hard-copy, audial, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University.

University Information Resource: any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

Policy

The Suffolk University community is encouraged to make innovative and creative use of information and technology in support of the University's mission of education, research and public service. University Information and/or University Information Resources are to be used exclusively to advance the University's mission, including but not limited to research, teaching, learning, enrichment, dissemination of scholarly information, and in connection with administrative activities, official University business or other University-approved activities. University Information Resources are limited and should be used carefully with consideration and respect for the needs of others.

The University acknowledges that occasionally, University Users use University Information Resources for incidental personal purposes. Such incidental, personal uses are permitted if they are not excessive, do not interfere with the performance of a faculty, staff, administrator or student's duties, do not interfere with the efficient operation of the University or its Information Resources and are not otherwise prohibited by law or this Policy or any other University policy.

Impermissible Use
University Information and/or University Information Resources may not be used or otherwise accessed for purposes which are unlawful, unethical, dishonest, damaging to the reputation or resources of the University, in violation of University policy, in violation of the requirements and standards set forth in the Suffolk University Written Information Security Program (WISP), inconsistent with the University's mission or likely to subject the University to liability.

Examples of impermissible use include, but are not limited to:

- Adversely affecting University Information Resources such as bandwidth, security, and/or performance
- Using University Information and/or University Information Resources to engage in activities that may harass, threaten or abuse others
- Using excessive amounts of storage
- Sending mass messages, junk mail, spam or other broadcast messages
- Sharing passwords to University systems
- Accessing University Information Resources for the purpose of viewing pornography or engaging in abusive conduct in a chat room or social media channel
- Tampering or degrading systems performance
- Sending, copying, storing or displaying copyrighted material, including illegally downloading or sharing music, movies, software or other files
- Introducing viruses, worms, Trojan Horses, spy ware, malware or other rogue programs or physically damaging systems
- Downloading, installing or running security programs or utilities that reveal or exploit weakness in the security of a system such as password cracking programs, packet sniffers, port scanners, unless authorized by the Information Security Officer or Chief Information Officer.

Violation of Policy

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the University.

Revision History

Version	Date	Responsible University Office	Approved By
1.0	09/14/10	Provost Office	Provost Barry Brown