OIT OPERATIONAL PROCEDURE

ACCEPTABLE USE POLICY

1. PURPOSE

This rule establishes University policies with regards to the Acceptable Use Policy at Stevenson University.

2. POLICY

2.1. Access

Access to STEVENSON UNIVERSITY's information technology resources is a privilege granted to STEVENSON UNIVERSITY users (faculty, staff and students) in support of their studies, instruction, duties as employees, official business with the University, and/or other University-sanctioned activities. Access may also be granted to individuals outside of STEVENSON UNIVERSITY for purposes consistent with the mission of the University.

With the exception of implicitly publicly accessible resources such as websites, access to STEVENSON UNIVERSITY information technology resources may not be transferred or extended by members of the University community to outside individuals or groups without prior approval of the appropriate faculty, staff member or administrator. Such access must be limited in nature and fall within the scope of the educational mission of the institution. The authorizing University official is expected to ensure that such access is not abused.

Gaining access to the University's information technology resources does not imply the right to use those resources. The University reserves the right to limit, restrict, remove or extend access to and privileges within, material posted on, or communications via its information technology resources, consistent with this policy, applicable law or as the result of University disciplinary processes, and irrespective of the originating access point.

It is expected that these resources will be used efficiently and responsibly in support of the mission of the University as set forth in this policy. All other use not consistent with this policy may be considered unauthorized use.

2.2. Data Security, Confidentiality and Privacy

STEVENSON UNIVERSITY users are responsible for ensuring the confidentiality and appropriate use of institutional data to which they are given access, ensuring the security of the equipment where such information is held or displayed, ensuring the security of any accounts issued in their name, and abiding by related privacy rights of students, faculty and staff concerning the use and release of personal information.

Electronic mail and computer files are considered the private property of Stevenson University for the exclusive use of its staff, faculty and students. Access to such files will generally require permission of the sender or recipient of a message or the owner of the account in which the material resides, court order, or by written authorization by VP level or higher of Stevenson University. However, in the event of a sanctioned University investigation for alleged misconduct, e-mail or files may be locked or copied to prevent destruction and loss of information. Users may employ methods to increase the privacy of their files, provided they do not violate any provision of this policy or degrade system/network performance.

Email transmitted over the internet is not considered secure and employees are prohibited from transmitting confidential information unencrypted in an email or email attachment.

All users of STEVENSON UNIVERSITY's information technology resources are advised to consider the open nature of information disseminated electronically, and should not assume any degree of privacy or restricted access to such information. STEVENSON UNIVERSITY strives to provide the highest degree of security when transferring data, but cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by others.

2.3. Electronic Information Retention and Disclosure

Original electronic materials on central computing equipment and/or copies may be retained for specified periods of time on system backups and other locations; however the University does not warrant that such information can be retrieved.

Unless otherwise required by law and/or policy, STEVENSON UNIVERSITY reserves the right to delete stored files and messages to preserve system integrity. STEVENSON UNIVERSITY also reserves the right to modify system parameters provided timely notice is provided to system users when appropriate. Except in an emergency, users will be given ample advance notice, taking the academic year calendar into account, to save any personal files and messages.

Electronic files or messages, whether or not created and stored on University resources, may constitute a University record subject to disclosure under the federal, state or local laws, or as a result of litigation. Electronic copies must be provided in response to a public record request or legally issued subpoena, subject to very limited exceptions, as with other documents created and retained by the University.

Disclosure of confidential information to unauthorized persons or entities, or the use of such information for self-interest or advantage, is prohibited. Access to non-public institutional data by unauthorized persons or entities is prohibited.

Requests for disclosure of confidential information and retention of potential evidence will be honored when approved by authorized University officials or required by state or federal law.

The university reserves the right to access, inspect, delete or disclose the contents of any files, documents, messages created or sent or stored or received using the computer systems or services of the university. This applies to both physical and electronic materials.

2.4. Network and System Integrity

In accordance with Federal , state and local laws and other policies and laws, activities and behaviors that threaten the integrity of computer networks or systems are prohibited on both University-owned and privately-owned equipment operated on or through University resources. These activities and behaviors include, but are not limited to:

2.4.1. Intentional or careless interference with or disruption of computer systems and networks and related services, including but not limited to the propagation of computer "worms,""viruses" and "Trojan Horses" and other activities that could have a negative impact on the STEVENSON UNIVERSITY computing environment in the judgment of the Vice President of Information Technology or designee.

2.4.2. Intentionally or carelessly performing an act that places an excessive load on a computer or network to the extent that other users may be denied service or the use of electronic networks or information systems may be disrupted

2.4.3. Failure to comply with authorized requests from designated University officials to discontinue activities that threaten the operation or integrity of computers, systems or networks

2.4.4. Negligently or intentionally revealing passwords or otherwise permitting the use by others of University-assigned accounts for computer and network access. Individual password security is the responsibility of each user. The user is responsible for all uses of their accounts, independent of authorization.

2.4.5. Altering or attempting to alter files or systems without authorization

2.4.6. Unauthorized scanning of ports, computers and networks

2.4.7. Unauthorized attempts to circumvent data protection schemes or uncover security vulnerabilities

2.4.8. Connecting unauthorized equipment to the campus network or computers. University authorized business and other activities directly related to the academic mission of the University are excluded.

2.4.9. Attempting to alter any University computing or network components, including but not limited to bridges, routers, hubs, wiring, and connections, without authorization or beyond one's level of authorization as designated by the administrator responsible for that equipment, i.e. the Vice President of Information Technology, or campus President or designee.

2.4.10. Utilizing network or system identification numbers or names that are not assigned for one's specific use on the designated system

2.4.11. Using campus resources to gain unauthorized access to any computer system and/or using someone else's computer without their permission

2.4.12. Providing services or accounts on University computers or via University networks to other users from a personal computer unless required to meet the normal activities of students working as individuals or in collaborative groups to fulfill current course requirements. University authorized business and other activities directly related to the academic mission of the University, are also excluded.

2.4.13. Registering a STEVENSON UNIVERSITY IP address with any other domain name for other than University business.

It is recognized that Information Technology programs have unique needs that may require exceptions from the restrictions within this Acceptable Use Policy. Because of these needs an Experimental Network, that is separate from the university-wide network, will be established and exempted from the restrictions of the Acceptable Use Policy except where state and federal laws are concerned. The Experimental Network will be governed by its own Acceptable Use Policy. Any Experimental Network traffic that passes outside the university firewall will be in compliance with the FIRN Acceptable Use Policy.

2.5. Commercial Use

Use of the University's information technology resources is strictly prohibited for unauthorized commercial activities, personal gain, and private, or otherwise unrelated to the University business or fundraising. This includes soliciting, promoting, selling, marketing or advertising products or services, or reselling University resources.

Campus auxiliary organizations are authorized to provide services and products to students, faculty and staff, and invited guests of the University through their operations. The University President or designee may authorize additional limited commercial uses. Such uses are excluded from the above prohibitions. These prohibitions are not intended to infringe on authorized uses that enable students, staff and faculty to carry out their duties and assignments in support of the University mission.

2.6. Fraud

Use of University information technology resources for purposes of perpetrating fraud in any form is strictly prohibited. Fraudulent activities include but are not limited to sending any fraudulent electronic transmission, fraudulent requests for confidential information and fraudulent submission and/or authorization of electronic purchase requisitions.

2.8. Harassment

Harassment of others via electronic methods is prohibited under Maryland Statutes and other applicable laws and University policies. It is a violation of this policy to use electronic means to harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference. It may be a violation of this policy to use electronic means to harass or threaten groups of individuals by creating a hostile environment.

2.9. Copyright and Fair Use

Federal copyright law applies to all forms of information, including electronic communications, and violations are prohibited under this policy. Infringements of copyright laws include, but are not limited to, making unauthorized copies of any copyrighted material (including software, computer code, text, images, audio, and video), and displaying or distributing copyrighted materials over computer networks without the author's permission except as provided in limited form by copyright fair use restrictions. The "fair use" provision of the copyright law allows for limited reproduction and distribution of published works without permission for such purposes as criticism, news reporting, teaching (including multiple copies for classroom use), scholarship, or research. The University will not tolerate academic dishonesty or theft of intellectual property in any form.

2.10. Electronic Communications

University electronic communications are to be used to enhance and facilitate teaching, learning, scholarly research, support academic experiences, to facilitate the effective business and administrative processes of the University, and to foster effective communications within the academic community. Electronic mail, news posts, chat sessions or any other form of electronic communication must comply with Maryland Statutes, Martland Educational Code, STEVENSON UNIVERSITY Policies and the Student Code of Conduct.

2.11. Web Sites

An official STEVENSON UNIVERSITY web page is one that is formally acknowledged by the chief officer of a University department or division as representing that entity accurately and in a manner consistent with STEVENSON UNIVERSITY's mission. Without such acknowledgment, a web site, regardless of content, is not "official." Official pages are the property and responsibility of the University or department that created them and follow the University (Novus) Web Style Guide and University Logo Guidelines "Unofficial" information may also be posted and maintained by individual faculty, staff and student organizations. STEVENSON UNIVERSITY does not undertake to edit, screen, monitor, or censor information posted by unofficial authors, whether or not originated by unofficial authors or third parties, and does not accept any responsibility or liability for such information even when it is conveyed through University-owned servers.

Both official and unofficial web sites are subject to the other provisions of this policy if they use University resources such as University-owned servers and the STEVENSON UNIVERSITY network to transmit and receive information.

2.12. Policy Compliance

The Assistant Vice President of Information Technology, or designee, is authorized by the President to ensure that the appropriate processes to administer the policy are in place, communicated and followed by the University community. The President or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate University officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

The President or designee will inform users about the policy; receive and respond to complaints; collect and secure evidence as required; advise and assist University offices on the interpretation, investigation and enforcement of this policy; consult with University Legal Counsel on matters involving interpretation of law, campus policy, or requests from outside law enforcement agencies and/or legal counsel; and maintain a record of each incident and its resolution to inform future policy changes.

2.13. Consequences of Non-Compliance

Enforcement will be based upon receipt by Office of Information Technology of one or more formal complaints about a specific incident or through discovery of a possible violation in the normal course of administering information technology resources.

First offense and minor infractions of this policy, when accidental or unintentional, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the resource. This may be done through e-mail or in person discussion and education.

Repeated offenses and serious incidents of non-compliance may lead to University disciplinary action under University disciplinary policies and procedures for students and employees, employee contract provisions where appropriate, private civil action, and/or criminal charges. Serious incidents of non-compliance include but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, copyright violations, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior.

In addition to the above, inappropriate use of Information Technology resources may result in personal criminal, civil and other administrative liability.

Appeals of University actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for STEVENSON UNIVERSITY students and employees.

2.14. Reporting Irresponsible or Inappropriate Use

The President or designee is responsible for reviewing violations of this policy and will act in accordance with University policies and guidelines for investigations and resolution of problems. Suspected infractions of this policy should be reported to the Vice President of Information Technology. Any employee may report a violation of this policy. The infraction must be reported to their immediate superior who may take those actions that are appropriate under this policy.

2.14. Revision History

Date	Description	
02/07/2011	Initial policy draft.	OIT
10/24/2013	Amended to clarify privacy.	OIT