Internet and Network Resources Acceptable Use Policy (AUP) 4.6-1

Details

Category:
Information Technology
Authorizing Body:
Vice President for Administration & Business Affairs – VP-ABA
Responsible Department:
Information Technology Services
Applies To:
Contractors & Vendors, Faculty, Lessees, Staff, Students, Visitors
Adopted Date:
05/02/1996
Revised Date:
06/05/2023
Print Policy

Table of Contents

Introduction/Purpose

Policy

User Responsibilities

General Regulations

Security and Privacy

Network Usernames and Email Accounts

Webpages

Wireless Routers/Access Points

Copyright

Procedures

Enforcement

Reporting Violations

Definitions

Related Policies & Forms

Appendix

Introduction/Purpose:

The purpose of the Internet and Network Resources Acceptable Use Policy (AUP) is to provide Users of the network resources guidance on their responsibilities, the general regulations regarding the network resources, information about security and privacy, the policies regarding network usernames and email accounts, webpage guidelines, personal wireless routers and access points, copyright, policy enforcement and how to report violations.

The University Information Technology Services (ITS) department manages the University Network (the Network). The University encourages faculty, staff, students, visitors, contractors & vendors to exchange information using the Network while reserving the right to monitor, manage and control its use. This policy is based on common legal, ethical, and professional standards. Adherence to this policy protects all Users and helps keep the Network a safe and rewarding place to navigate.

Users must not violate this Acceptable Use Policy (AUP) or local, state and federal laws while using the Network.

Policy:

User Responsibilities

These responsibilities have been established to protect Users from fraud and to ensure a safe and harassment-free computing environment.

1. Users are responsible for their use of the Network and computer equipment, and for protecting their username and password.

2. Each User is issued a single username and password that gives them access to the Network, Office 365, etc.

3. Users are responsible to report unauthorized use of their username to the Information Systems Security Manager or Executive Director of ITS. Using the Network without permission or failing to report unauthorized use can be a violation of federal and state law.

4. Users are responsible for safeguarding their own and others' personal information. They should not enter or send personal information such as usernames, passwords, date of birth, social security number, driver's license, credit card numbers, or medical/health data in email, electronic meeting notices/appointments, attachments, chat rooms or instant messages (IM), or to unsecure websites. They should not save or store such personal information on any electronic media or format including local hard drives or images without consulting with ITS staff regarding security.

5. Users are responsible for knowing the University's Harassment Policy. Employees see: SVSU Operations Manual (/operationsmanual/). Students see: Anti-Discrimination/Harassment Policy (/operationsmanual/legalcompliance/anti-harassmentdiscriminationpolicy25-2/).

6. Users are responsible for respecting copyright. For additional information refer to the Copyright section below and the SVSU Copyright Policy (/operationsmanual/academicresearch/copyright10-6/) in the SVSU Operations Manual (/operationsmanual/).

General Regulations

Users will respect the privacy and security of the Network, other users, other entities, and the intended use of the Network. Individual units or departments may set up additional guidelines that go beyond, but do not take the place of these regulations.

1. Users must not:
   - Use or attempt to use someone else's username and password
   - Give their own username and password to anyone
   - Use their own username and password to log someone else on

2. Users must not download and/or install copyright protected software, videos, images, data, music or any other material from any source, including peer to peer and shareware networks, unless the User

has (a) written permission from the author to use the material, (b) purchased the material from the product owner or a business with authorization to sell the copyrighted material, or (c) complied with the educators fair use guidelines of the Copyright Act of 1976 (see SVSU Copyright Policy (/operationsmanual/academicresearch/copyright10-6/) or Copyright below).

3. Users must not send unsolicited messages (junk or spam), forged messages, messages that will intimidate or harass other Users, or use network server space in a way that interferes with the efficiency of the Network. Users must not send numerous repeated messages, transactions or emails to another user or site "denial of service attack".

4. Users must not intentionally damage, alter or bypass software, hardware or Network components.

5. Users must not use the Network for partisan political activities, revenue-generating advertising, promoting business not related to the University, or personal business.

6. Users must not harass, threaten, or intimidate other University or non-University Users. Users must comply with all University rules regarding harassment and discrimination.

7. Users must not misrepresent their identity or relationship to the University when obtaining a University username or other Network services.

8. Users must not search for information on, get copies of, or change files of passwords or security settings belonging to the University or other Users or entities.

9. Users must not search for, use, or distribute information on the Network architecture, hardware or software components, databases, computer equipment, security components, or security bypass techniques of the University, or any other entity.

10. Users must not use any University or personal computer equipment or device connected to the Network to initiate, plan, produce, install or run programs that attempt to:

- Bypass or disable any Network security, registration, management system or device
- Bypass the encryption, licensing or delivery control of any licensed product in any form or media
- Damage or use excessive resources on the Network or anywhere on the internet
- Upload computer viruses, Trojan Horses, worms or a distributed "denial of service attack"

11. Users may connect personal devices to the Network. Users are responsible for ensuring that they have the appropriate anti-virus and malware protection on their devices. If the device causes issues to the Network, ITS reserves the right to isolate the problematic device. Gaming systems, personal entertainment systems (e.g., Roku, Chromecast, etc.) and wireless printers are allowed to be connected in student housing. Wireless printers must be connected to the SVSU wireless network and will be configured not to broadcast their own SSID. Wireless printers broadcasting their own SSID must be disconnected from the SVSU network immediately upon notification from ITS. No other non-SVSU supplied devices (e.g., network attached storage, wireless routers, etc.) are allowed to be connected to the Network unless approved by ITS in advance.

12. Users must not publish course content or course work in whole or in part, no matter what the medium, prepared by other Users to web sites without the express written consent of the author. This includes, but is not limited to, comments, lecture notes, papers, audio, video, and research.

13. Users must not promote illegal activity or material that negatively affects the University, or distribute copyrighted, pornographic or licensed software or material.

14. Employees must use the Network in a manner consistent with the University's instructional, public service, research, and administrative mission. The Network may not be used for personal business or personal gain except as permitted by other University policies or explicitly stated in University contracts.

15. Users are responsible for safeguarding personal information that they use in the performance of employment.
    - Users will not transmit documents or files with personal information across the Network or internet without using encryption.
    - Users that store documents and files with personal information must store them on approved University storage locations.
    - Users will not store documents and files with personal information on local hard drives, portable data storage media, or cloud destinations such as, but not limited to, Dropbox, Google Drive or Apple iDrive.

Security and Privacy

The University uses safety measures to protect the security of the Network, computer systems and User accounts. Users should be aware that the University cannot guarantee security and confidentiality. Users should exercise safe-computing practices by guarding their username, password and personal information.

1. Users should be aware that their University messages, sent or received, in connection with University business may be considered public records and may be disclosed to members of the public upon

request.

2. Users should be aware that their University address may be listed in University directories.

3. Users should be aware that their use of the Network and computer system is not private. The University does not regularly monitor individual use, but the normal operation, maintenance and fine-tuning of the Network require:

   - The back-up and caching of all forms of data and internet communications
   - The logging of activity
   - Use patterns to be checked
   - Other actions necessary for the delivery of service

4. Users should be aware that their Network and computer activity, including the content of individual communications, may be monitored without notice when:

   - Users have voluntarily made them available to the public.
   - It is necessary to protect the reliability, security or operation of the University, the Network and computer systems, or to protect the University from liability.
   - There is concern that the User has violated or is violating this policy.
   - Users appear to be engaged in unusual or uncommonly excessive activity.
   - It is required by law.

5. Users should be aware that the University may disclose the results of any general or individual monitoring, including the contents and records of individual communications, to the proper University staff or police agency, or use them in University disciplinary proceedings (see Enforcement below).

Network Usernames and Email Accounts

University-approved policies for issuing, limiting, or disabling usernames, email accounts, and internet or computer system use are explained through the SVSU Information Technology Services Policies.

1. University students and employees are automatically issued a University Username and email account. Alumni and retirees (those requesting an email account after retirement) may keep an email account per the following guidelines:
    - Upon graduation or retirement, an individual's SVSU account will transition to an email-only account. The SVSU email account will continue if the alumnus/retiree makes the required annual password change. Notifications are sent prior to password expiration. If the password is not changed the account will be terminated. Once the account is terminated, the mailbox and all messages will be removed from the system and not recoverable.
    - Multi-Factor Authentication (MFA) will be enforced on all active alumni and retiree email accounts.

2. The University reserves the right to stop incoming mass mailings (spam) without informing the sender or intended recipient.

3. The University reserves the right to regularly send out general information through University email. Email is the main method used to communicate University information, including financial aid awards and academic standing. Refer to the Student Email Communication Policy.

4. Employees shall not create email rules or processes in their SVSU email account that automatically forwards emails outside of the SVSU email system.

5. The University reserves the right to maintain lists of University email addresses. The lists are only used to distribute information and are not available or sold to any outside company.

Webpages

It is the policy of the University to ensure its web sites correctly represent Saginaw Valley State University and its mission.

1. All official SVSU webpages must:

   - Comply with all laws governing copyrights, intellectual property, libel, and privacy
   - Not violate any policy, rule or regulation of the University
   - Not be used for non-SVSU commercial activities
   - Comply with Americans with Disabilities Act standards

2. The University owns and has exclusive rights to all official webpages and the digital assets published under the svsu.edu domain; and any such webpages stored on servers or devices owned or leased by, or contracted for, the University.

3. Faculty, staff, and students may create personal webpages for use in their various academic and administrative duties and activities and may publish on SVSU's web servers. Personal webpages are not considered official SVSU webpages. The contents of an individuals' webpage published on SVSU's servers must comply with the University's Acceptable Use Policy and adhere to University standards when using University logos and/or graphics.

4. Except for approved University-related items, sale of goods and services is prohibited on any SVSU site. Non-SVSU advertising, merchandising and commercial activities are prohibited in the svsu.edu

domain.

5. University web pages must not contain links to commercial web sites unless those companies are corporate sponsors or partners of the University. Links to non-commercial sites are permitted only if the content of those sites comply with the University's Acceptable Use Policy.

6. ITS reserves the right to disable a website that belongs to a club, organization, employee, or student if a security vulnerability is found or for other reasons as deemed appropriate by the University. The site may, at the University's sole discretion, be restored if the owner corrects the vulnerability.

Wireless Routers/Access Points

The University does not allow personally-owned routers or wireless access points to be installed anywhere on campus or in student housing. For more detailed information, please contact the ITS Support Center.

Copyright

Refer to SVSU Copyright Policy for additional information on copyright.

Using the Network to copy, store, display or distribute copyrighted material (licensed software programs, data, images, music or any other materials) without the permission of the copyright owner, except as otherwise allowed under the U.S. Copyright Law, is prohibited. See these sites for additional information including fair use of copyrighted material:

- U.S. Copyright Office (http://www.copyright.gov/)
- Educators, Technology and the Law (http://horizon.unc.edu/projects/resources/educators.asp)
- Recording Industry Assoc. of America (http://www.riaa.com/)

Under the Digital Millennium Copyright Act, the University is obligated to take appropriate enforcement action if it receives a complaint that unauthorized copyrighted material is published or downloaded on the Network.

To report online copyright infringement or violations, notify the University's agent in accordance with the U.S. Online Copyright Infringement Liability Limitation Act (OCILLA).

Procedures:

Enforcement

Various methods are used to enforce this policy ranging from warnings, loss of privileges for visitors/guests, expulsions for students and termination of employees.

Violations of the law will be reported to the appropriate authorities.

Reporting Violations

Report violations of the University's Acceptable Use Policy to the Executive Director of ITS or your supervisor. Depending upon the nature and severity of the violation, the Executive Director of ITS or a designee, shall refer the matter for appropriate action.

Definitions:

Users – Any faculty, staff, student, visitor, contractor, or vendor provided access to SVSU's network resources.

Related Policies & Forms:

SVSU Information Technology Services Policies (https://svsu.teamdynamix.com/TDClient/1949/Portal/KB/?CategoryID=15592)

Copyright Policy 1.0-6 (http://www.svsu.edu/operationsmanual/academicresearch/copyright10-6/)

Student Email Communication Policy 4.6-2 (http://www.svsu.edu/operationsmanual/informationtechnology/studentemailcommunicationpolicy46-2/)

Anti-Harassment/Discrimination Policy 2.5-2 (http://www.svsu.edu/operationsmanual/legalcompliance/anti-harassmentdiscriminationpolicy25-2/)

Appendix:

Digital Millennium Copyright Act

Online Copyright Infringement Liability Limitation Act (OCILLA)