SEWANEE
THE UNIVERSITY OF THE SOUTH

Acceptable Use Policy

Purpose

The University of the South's information technology (IT) resources exist to support the academic and administrative activities needed to fulfill the University's mission. Access to these resources is a privilege that should be exercised lawfully and in accordance with other applicable University policies and guidelines by faculty, staff, students, other stakeholders of the University and its guests.

The purpose of this policy is to outline the acceptable use of technology resources at the University of the South and the expectations to help protect the information assets of the University.

Scope

This policy applies to all users of University owned, managed, or otherwise provided IT resources. Individuals covered by this policy include, but are not limited to all employees, students, contractors, alumni, volunteers, consultants, and service providers with access to the University's IT resources and/or facilities. Individuals are also subject to any federal, state and local laws governing their use of these resources. This policy is subject to change at the discretion of the University.

Definitions

Term	Definition
Chief Information Officer (CIO)	Role held by the Associate Provost for Library and Information Technology Services is known as the CIO. The CIO is a member of the vice-chancellor's cabinet and is responsible for all aspects of Library and Information Technology Services for the University.
Information Technology (IT)	Information Technology is part of the Library and Information Technology Services (LITS) division of the university. IT is charged with establishing, monitoring, and maintaining information technology systems and services. IT includes the Technology, Access, & Support (TAS) department and the Strategic Digital Infrastructure (SDI) department.
Information Technology (IT) Resources	Includes all the University owned, licensed, or managed hardware and software, email domains and related services, and any use of the University's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.
LITS	Library and Information Technology Services is a division of the University that encompasses the library and information technology functions of the University.

Stakeholder	A stakeholder is a person with an affiliation with the University. This includes students, faculty, staff, alumni, retirees, community members, leaseholders, contractors, visitors, volunteers, and others.

Policy

Access to and use of information technology (IT) resources at the University are privileges extended to stakeholders of the University and its guests. University wide guidelines such as handbooks, policies, community standards, the mission of the University, as well as federal, state, local and international laws/regulations apply to the responsible use of IT resources.

1.0 Security

All users and administrators of the University's IT resources are expected to be mindful of the security of these resources and adhere to the University's Information Security Policy. Users and administrators are also reminded to:

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Use encryption when transmitting sensitive files.
- Exercise caution and good judgment when opening email attachments or following links in emails. Whether the sender is known to the user or not, these attachments may contain viruses, spyware or other malware.

2.0 Personal Use

The University acknowledges that occasionally stakeholders use University resources for noncommercial, personal use. Such occasional noncommercial uses are permitted, if they are not excessive, do not interfere with the performance of their University responsibilities, do not interfere with the efficient operation of the University or its IT resources, and are not otherwise prohibited by any University policy or directive or law.

3.0 Impermissible Uses

The University's IT resources may only be used for legal purposes and may not be used for any of the following purposes or any other purposes that are illegal, dishonest, damaging to the reputation of the University, inconsistent with the mission of the University, or likely to subject the University to liability. Impermissible uses (some of which may constitute illegal uses), include but are not limited to the following:

- Fraudulent and Illegal Use
    - Harassment
    - Retaliation
    - Libel or slander
    - Fraud or misrepresentation
    - Unauthorized copy or transmission of copyright protected material
    - Violation of the rights of any individual or company involving information protected by copyright, trade secret, patent or other intellectual property
    - Violation of software license agreements by installing or distributing pirated or other software products that are not appropriately licensed for use the University
- University Standards
    - Academic dishonesty
    - Use of the University's trademarks, logo, insignia, or copyrights without prior approval
    - Use of the IT resources for private business purposes unrelated to the mission of the University or to University life

    - Use the same password for University accounts as for other non-university accounts (for example, Facebook, personal email, etc.)
    - Violation of privacy
    - Viewing, posting or sending pornographic, sexually explicit, or offensive material
    - Posting or sending material that is contrary to the mission and values of the University
    - Hosting of a server outside of the SDI department's environment unless approved by the CIO or designee. For example, a gaming server, web server, chat server, etc.
- E-mail
    - Develop or use an unapproved mailing list for email solicitations
    - Send unsolicited e-mail messages, including "junk mail" or other advertising material to individuals who did not specifically request such material
    - Use or solicit an email address with the intent to harass another
    - Create or forward chain letters or messages
- Impersonation
    - Circumventing user authentication or security of any host, network or account
    - Unauthorized use of computer accounts, access codes, passwords, network identification numbers, or email addresses assigned to others
    - Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information
    - Create and/or use a proxy server of any kind, other than those provided by the University, or otherwise redirect network traffic outside of normal routing
    - Use any type of technology designed to mask, hide, or modify their identity or activities electronically
- Confidentiality
    - Executing any form of network monitoring which will intercept data not intended for you
    - Effecting a security breach. Security breaches include, but are not limited to, accessing data for which the person is not an intended recipient or logging into a server or account the person is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Malicious Activity
    - Destruction of or damage to equipment, software or data belonging to the University or others
    - Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends
    - Make copies of another user's files without that user's knowledge and consent
    - Disruption of electronic communications. For purposes of this section, "disruption" includes, but is not limited to, networking sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
    - Port scanning or security scanning of either the University's network or any other external network unless prior approval has been obtained from the Associate Provost for Library and Information Technology Services
    - Intentional or negligent distribution of computer viruses, ransomware or other malware
    - Intentionally develop or use programs to infiltrate a computer or network and/or damage or alter the software components of a computer or network
    - Install, attach, or connect wired or wireless network switches, routers or access points to redirect traffic without the knowledge and permission of the IT staff
- Political Activity
    - Use any of the University's IT resources in a way which suggests University endorsement of any political party, candidate, campaign, political activity, fundraising or influencing legislation.

- Any other use of the University's IT resources with respect to political activity must be permitted by applicable University policy and consistent with applicable laws.

4.0 Reporting Violations
All users should report any discovered unauthorized access attempts or other improper usage of University owned or provided computers, networks, applications, or information. If you observe, or have reported to you, a security or abuse problem with any University computer or network facilities, including violation of this policy, you should notify IT by emailing IT-SECURITY@sewanee.edu, contacting the CIO, the Office of Human Resources or other appropriate administrator.

5.0 Exceptions
Exceptions to the policy may be granted by the Chief Information Officer.

6.0 Related Policies
- Information Security Policy
- Education Records and FERPA Policy

7.0 Consequences
All University employees, students, retirees, alumni and other stakeholders using University IT resources are expected to abide by this policy. Violations of this policy may be treated as violation of University policy and/or violations of civil or criminal law. Any employee who violates this policy may be subject to disciplinary action, up to and including termination of employment. Any student who violates this policy may be subject to disciplinary action, up to and including suspension from the University. Others who violate this policy may have their access suspended, blocked or terminated. Concerns about unlawful activity will be referred to the appropriate law enforcement agency.

8.0 Responsibilities
All University stakeholders are responsible for understanding and abiding by this policy. The Library Information Technology Services Division, particularly the CIO, the Strategic Digital Infrastructure (SDI) and Technology, Access and Support (TAS) departments, is responsible for maintaining this policy.
The University reserves the right to protect, repair and maintain the University's technology resources and network integrity. In accomplishing this goal, The University, and any applicable contracted vendors must make every reasonable effort to respect a user's privacy. However, stakeholders do not acquire a right of privacy for communications transmitted or stored on University resources. Any information obtained about a user through routine maintenance of the University's computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with acceptable or lawful use of the University's technology resources.

9.0 Policy Authority
This policy is maintained by the Associate Provost for Library and Information Technology Services for The University of the South

10.0 Revision History

Version	Date	Author	Revisions
1.0	September 21, 2022	Various	Initial Policy