Acceptable Use Policy

Purpose

Saint Leo University recognizes that Saint Leo University personnel roles differ and that it can be challenging to define all acceptable and unacceptable behaviors related to the use of Saint Leo University technology. The purpose of the Acceptable Use Policy is to define the requirements for the acceptable use of information resources at Saint Leo University.

Audience

All Saint Leo University employees, consultants, contractors, and sub-contractors, have a personal responsibility to protect Saint Leo University's Applications and Data from intentional or accidental misuse and unauthorized disclosure.

Policy Exceptions

Exceptions to this policy must be formally documented and approved by the Vice President of Business Affairs.

Policy Violations

Violating this policy will result in disciplinary action, up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company reserves the right to report such activities to the applicable authorities.

Policy Information

Policy #	Policy Statement	Reference
General		
1.1	Members of the Saint Leo University community (employees, students, visitors, and contractors), have **no** expectation of privacy when utilizing university-computing resources. The university reserves the right to inspect, without notice, the contents of computer files, regardless of medium, the contents of electronic mailboxes and computer conferencing systems, systems output, and to monitor network communication.	N/A
1.2	Use of Saint Leo University technology must comply with local, state, and federal laws related to issues such as copyright, trademark, insider trading, harassment, and discrimination.	N/A
1.3	Saint Leo University reserves the right to audit and monitor activities that involve Saint Leo University technology including the monitoring of e-mail and Internet activity, and to restrict access to certain websites. Such monitoring and other activities are subject to, and compliant with, local legal and regulatory requirements.	N/A
1.4	Saint Leo University reserves the right to revoke the access of any employee, at any time, if the individual fails to use the Saint Leo University technology appropriately.	N/A
1.5	All non-public information should never be sent or posted on the public Internet. The information we use and share within Saint Leo University is sensitive and confidential; the inappropriate disclosure of this information could damage the reputation of Saint Leo University, the reputation of its customers, and Saint Leo University relationship with its customers.	N/A
1.6	Sensitive information (Personally identifiable information, University proprietary information, health records, student records etc.…) As deemed by the Data Classification policy must not be displayed in an open environment. Physical documents or electronic images must be secured when not actively being used. Always clear your workspace of any Sensitive information when leaving your desk.	N/A
Authorized Users		

2.1	An authorized user is any person who has been granted authority by Saint Leo University to access its computing, network, information, or telephone systems. Unauthorized use is strictly prohibited.	N/A
2.2	Prior to accessing Saint Leo University network or using Saint Leo University-owned / leased equipment, Saint Leo University employees must have completed a formal acknowledgement form agreeing to Saint Leo University Policies and Standards with respect to any such asset, as well as with respect to any information or communication stored, processed, or transmitted over such asset.	
2.3	Whenever a user ceases being Saint Leo University employee, or if a user is assigned a new position and/or responsibilities, use of technology resources for which they are not specifically authorized in their new position or circumstances shall cease.	N/A
2.4	Authorized users must not share credentials (user name and password) with others. Contact DIT immediately if you suspect your user account (password) has been compromised.	N/A
Loss and Theft		
3.1	Lost or stolen equipment must immediately be reported to your supervisor, and DIT.	https://helpdesk.saintleo.edu
3.2	Confidential information in physical or electronic format believed to be lost or stolen must be reported to your supervisor and Saint Leo Department of Information Technology.	https://helpdesk.saintleo.edu
Illegal Activities		
4.1	Under no circumstances are Saint Leo University employees authorized to engage in any activity that is illegal under local, state, or federal law while using Saint Leo University resources.	N/A
Internet		
5.1	Saint Leo University reserves the right to block certain non-business related websites, category of websites from time to time as deemed necessary and without notification to the Saint Leo University user community.	N/A
5.2	Saint Leo University reserves the right to retain information gathered on Internet usage.	N/A
5.3	Only authorized individuals are permitted to express corporate positions on behalf of Saint Leo University on any site.	N/A
5.4	Accessing inappropriate or offensive material (pornographic in nature) violates the university's Sexual harassment policy and is prohibited	N/A
5.5	Access to on-line gambling is prohibited on the Saint Leo University Network.	N/A

5.6	Peer-to-Peer (“P2P”) networking and file sharing is not allowed on the Saint Leo University network or systems under any circumstances.	N/A
5.7	Downloading any anonymizer, such as Tor, on any Saint Leo University owned device, or use of the Tor network over company networks is expressly prohibited.	N/A
5.8	Personal use of Saint Leo University network systems is permitted, as long as such usage does not negatively affect Saint Leo University and does not negatively affect the user's job performance.	N/A
Electronic Communication		
6.1	Personal use of Saint Leo University communications systems is permitted, as long as such usage does not negatively affect Saint Leo University and does not negatively affect the user's job performance.	N/A
6.2	Information that is considered Institutional or Confidential by Saint Leo University should not be sent via email, regardless of the recipient, without proper authorization and technical controls.	N/A
6.3	The use of encryption to protect sensitive information during transmission is required to comply with Saint Leo University Policies, Standards, and applicable laws.	N/A
6.4	The Saint Leo University email system must not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.	N/A
6.5	Saint Leo University email must not be automatically forwarded to an external destination.	N/A
6.6	Saint Leo University employees who receive unsolicited email or web requests for sensitive information are prohibited from sharing or disclosing any such information to any party outside of Saint Leo University.	N/A
Telecommunications		
7.1	Personal usage of Saint Leo University telecommunications systems is permitted during, before, and after business hours, as long as such use follows pertinent policies and guidelines and does not have a detrimental effect on Saint Leo University, its customers, or on the user's job performance.	N/A
7.2	A personal identification number (PIN) must protect Voicemail boxes.	N/A
Modems		
8.1	Use of external modems or wireless access points are not permitted to connect to the Saint Leo University network unless approved by DIT.	N/A
8.2	Mobile broadband modems must not allow split tunneling when connected to the Saint Leo University network.	N/A

8.3	Traditional modems are only permitted when no other, more secure method is available to access the data or system and approved by the Saint Leo Department of Information Technology.	N/A
Software		
9.1	No unapproved software is to be installed on Saint Leo University-owned information systems without approval by Saint Leo Department of Information Technology.	Client Computing Security Policy
9.2	Peer-to-Peer ("P2P") networking and file sharing software is prohibited from being installed on any Saint Leo University owned device.	N/A
Portable Media		
10.1	Files containing Confidential or Internal Use data may not be stored on mobile media or mobile devices unless protected by Saint Leo University approved encryption solutions.	N/A
10.2	Confidential or Internal Use data must never be stored on a personal mobile device unless it is protected by a Saint Leo University approved solution.	N/A
Misuse Reporting		
11.1	Saint Leo University personnel should report actual or suspected misuse of Saint Leo University resources to the Department of Information Technology.	https://helpdesk.staintleo.edu
Social Media		
12.1	Saint Leo University employees are prohibited from revealing any sensitive information when engaged in any public communications.	N/A
12.2	Saint Leo University reserves the right to review and remove comments that are deemed inappropriate from Saint Leo University sponsored social media.	N/A
Circumvention of Security		
13.1	Unless required for Saint Leo University business purposes and approved by Department of Information Technology, Saint Leo University personnel may not attempt to circumvent or subvert the security provisions of any Saint Leo University system.	N/A
13.2	Saint Leo University employees must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security, unless specifically authorized by the Information Security Group.	N/A
Prohibited Systems and Network Activities		
14.1	Users must not access, modify, or delete other users' files or system settings without express permission.	N/A
14.2	Deliberate attempts to tamper with or degrade the performance of a Saint Leo University computer system, telephone system, or network, or to deprive authorized users of access to or use of such resources are prohibited.	N/A

14.3	Using the network in support of groups outside the University when such use is not in keeping with the mission of the University.	N/A
14.4	Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, a user's working computer session, via any means, locally or via the Internet or network.	N/A
14.5	Port scanning, security scanning, and password cracking are expressly prohibited.	N/A
14.6	Performing any form of network monitoring that intercepts data not specifically intended for the personnel's host is prohibited.	N/A
Privacy of Stored Personal Information		
15.1	Saint Leo University personnel do not have any expectation of privacy in anything they store, send, or receive on Saint Leo University information systems.	N/A
15.2	Saint Leo University may monitor or review information system usage and files, including content, without prior notice.	N/A
15.3	Saint Leo University reserves the right to actively monitor, restrict, use, and dispose of email messages, other electronic communications, and/or personal stored files.	N/A
15.4	Saint Leo University personnel should exercise caution when storing and processing personal and sensitive information not directly related to Saint Leo University business.	N/A
Privacy of Personal Electronic Communications		
16.1	Saint Leo University employees do not have an expectation of privacy in anything they store, send, or receive on Saint Leo University information systems. All messages sent over Saint Leo University computer and communications systems are subject to monitoring and review in the interest of protecting the security of Saint Leo University information.	N/A
16.2	To properly maintain and manage the security of information resources, Saint Leo University reserves the right to examine all information stored in or transmitted by these information systems.	N/A
Electronic Monitoring Areas		
17.1	Individuals are subject to electronic monitoring while on Saint Leo University premises and in secure areas. This monitoring is used to measure policy compliance as well as to protect Saint Leo University, its personnel, and others. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no visual or audio monitoring will be performed without the express consent of the leadership team and legal consultation.	N/A

Contact Information

If you have any questions about this policy, you can contact us:

Saint Leo University
Department of Information Technology
Web: https://helpdesk.saintleo.edu
Phone: (352)588-8888

Document REF	
Version	1
Effective Date	06/01/2016
Document Author	Information Security Team
Document Owner	Information Security Team

Revision History

Revision Level	Date	Description	Change Summary
1	05/17/2021	Review	
2	05/02/2025	Review	

Approval

Name	Position	Signature	Date
Steven Carroll	CIO	Steven Carroll	05/05/2025