IT POLICIES OF SRI SAI RAM INSTITUTE OF TECHNOLOGY

I General IT Ethics / Ethos Policy

Purpose

Sri Sai Ram Institute of Technology is an educational institution, which encourages continuous learning, experimentation, and the development of the adult learner. The College is dedicated to respect privacy and freedom of individuals and expects each individual to act in a responsible, legal, ethical and efficient manner when using information technology systems and resources of the college. These systems are designed to encourage high-quality educational, professional and career development and self-discovery & research activities.

The purpose of this policy is to define responsible and ethical use of information technology resources available at Sri Sai Ram Institute of Technology that guides faculty, student, and staff.

Statement of Policy

Sri Sai Ram Institute of Technology provides access to information technology resources for faculty, staff, students, and certain other users to support the mission of the college. Every authorized user of information technology resources at college is responsible for utilizing these resources in an efficient, ethical, and legal manner and in ways consistent with overall college policy.

Scope

The following principles serve to guide the responsible use of information technology for all the users of college.

1. Respect the rights of others by complying with all college policies regarding sexual, racial and other forms of harassment, and by preserving the privacy of other individuals. For example, it is prohibited to send harassing messages via email or social networking or transmit or reveal personal or private information individuals.

2. Use computing facilities, accounts and data only when you have appropriate authorization and use them for approved purposes. For example, you should not use Information Technology resources of "Sri Sai Ram Institute of Technology" to run a business or to access another individual's computer account.

3. Respect all pertinent licenses, contractual agreements and copyrights. Use only legal versions of copyrighted software in compliance with vendor license requirements. For example, you should not post another individuals copyrighted material on your web page or install software with a single user license on multiple computers.

4. Preserve the integrity of computing systems, electronic data, and communication networks. For example, one should not modify settings on a desktop computer to make it unusable for others or excessively utilize network resources, like music videos, which might overload college network bandwidth.

5. Respect and adhere to all appropriate local, state and government laws. For example, it is prohibited to use IT resources of the college to attack computers on another network by launching viruses, worms, or other forms of attack.

Privacy

While the College values and respects the privacy of its staff, faculty, students, and other users, the intrinsic nature of electronic records limits the extent to which the College can guarantee a user's privacy. Despite security protocols, communications over the Internet—and across the local campus network of the college—can be vulnerable to interception and alteration. Consequently, the College cannot assure that absolute privacy can be maintained for data that resides on the College network or on storage media.

Out of respect for personal privacy, the College does not routinely examine the contents of data or files in user accounts. However, on occasion, circumstances may require an examination of a user's files to maintain system security, to administer or maintain system integrity, to access necessary College information or in response to legal mandate. In such cases, authorized personnel may examine a user's data without notice. Authorized personnel are those specifically entrusted and approved by the College Principal.

Personal Use

Personal use is defined as the non-academic, non-administrative use of IT systems of the college. Such use is solely discretionary; it neither serves an essential employment function nor is it related to academic discourse. Data that result from personal use are "personal data".

Personal use of IT resources of the college is secondary for performing essential College functions using such resources. If personal use of College IT resources interferes with or causes disruptions to the essential functions of the College performed by IT, then authorized personnel may curtail such use.

Passwords and User IDs

System accounts, passwords, and user IDs plays an important role in protecting the files and privacy of all users. Because users are responsible for all uses made of their accounts, users must take exceptional care to prevent unauthorized use of their accounts. This includes changing passwords regularly and disabling "automatic" log-ins.

In most cases, it is inappropriate—and perhaps dangerous—to allow another person to use another user's network credentials or email account. In some cases, a user's data are vulnerable to alteration or deletion. In others, the validity of a user's credentials could be compromised. Alternatively, if criminal activity can be traced to a user's account, the person to whom the account is assigned may be held accountable. The College, therefore, reserves the right to restrict or prohibit password sharing.

Data Storage and Back-ups

The College maintains a centralized repository of data stored in user accounts on the College network. This includes all the data that a user creates and saves on the College's network storage devices. It also includes saved email messages, attachments, files, and folders.

The College reserves the right to restrict the amount of network storage available for users. This includes the prerogative to impose quotas on the number and/or size of stored files.

Data files are routinely backed up on a daily, weekly, monthly, and/or yearly basis. These back-ups facilitate the restoration of College data that have been lost, altered, or damaged. The College will not routinely retrieve backed-up personal data. Users, therefore, are encouraged to maintain independent back-ups of their important personal data, including email messages. Sri Sai Ram Institute of Technology disclaims any responsibility for maintaining or providing access to backups of a user's personal data.

In case of data backed up by the IT department, retrieval or restoration of the same will be the discretion of the Principal.

Security

The College implements appropriate "industry-standard" practices concerning the security of the IT resources of the college. These methods are designed to protect against unauthorized access, intrusion, or damage to the availability, access, or integrity of the IT systems of the college. However, primarily due to the nature of security threats and the remote possibility of a breach of security, the College warrants neither a user's privacy nor the integrity of data stored on the College network (since the College has already adhered to all the industry norms of standards of security)

Copyright, Trademark, and Domain Names

Users must comply with all copyright, trademark, and other intellectual property laws. In general, permission is necessary for a user to reproduce materials, such as video, music, images, or text. To "reproduce" in this context includes downloading and saving a digital copy to a hard drive or other storage media. Photocopying copyrighted materials without authorization is also prohibited.

In addition, users must generally obtain permission from the copyright owner to prepare derivative works, including modifying existing works. Copyright law also prohibits the distribution, display, or performance of works created by another without a proper release.

Additionally, the College owns certain Internet domain names. These include sairamit.edu.in, sairamgroup.in and other such domain names. Registration of domain names incorporating or referencing College trademarks is prohibited without the approval of the college Principal.

Compliance and Enforcement

All users of IT resources of the college must abide by these policies. Users not wishing to agree to and comply with this policy will be denied use of or access to IT resources of Sri Sai Ram Institute of Technology.
College community users who intentionally violate these policies are subject to disciplinary action by the College, in line with the duly established processes of the College. On the discretion of the Principal the alleged violations of this IT policy may be referred to the College disciplinary body. In addition, the Principal may conduct an investigation regarding the alleged infraction. Violators may also be liable for civil damages and/or criminal prosecution, if applicable.

Guest users of publicly available IT resources of the college are also subject to the terms of this policy. While explicit acceptance of this policy is not required for guests to access these limited IT resources, guests are accountable for their actions while using College IT resources. Guests who violate this policy will be asked to cease use and may be barred from further access.

Members of the "Sri Sai Ram Institute of Technology" community who believe they have witnessed or been a victim of a violation of this policy should notify or file a complaint with the appropriate authority at the College office. Students should report suspected violations to the Class Counselor. Faculty members should report suspected violations to the Principal. Staff members should report suspected violations to their department head that may further report the problem to the Discipline Committee. Reports of suspected unauthorized use or misuse of "Sri Sai Ram Institute of Technology" information technology resources would be investigated pursuant to standard College procedures.

II Data Security Policy

Purpose

This policy defines the guidelines for the security and confidentiality of data maintained by Sri Sai Ram Institute of Technology, both in paper and electronic form. This policy also informs each person who is entrusted to access student, employee and/or institutional data of their responsibilities with regard to confidentiality and safeguarding the data of Sri Sai Ram Institute of Technology.

Statement of Policy

All custodians and guardians of administrative data are expected to manage, access, and utilize the data in a manner that maintains and protects the security and confidentiality of that information. All notice to the Government of India, State & local regulations must be considered and adhered to when using or sharing personal or confidential information. Any notice of a breach of confidential information whether in paper or electronic form MUST be reported to the Principal.

Under no circumstances shall credit card numbers be stored or sent from College servers or desktops.

Scope

College employees, or others who are associated with the college, who request, use, possess, or have access to college administrative data must agree to adhere to the protocols outlined in the general IT policy.

Changing data of oneself or others except as required to fulfill one's assigned College duties or as authorized by a supervisor. (This does not apply to self-service applications that are designed to permit you to change your own data).

- Disclosing information about individuals without prior authorization by the college administration.
- Engaging in what might be termed "administrative voyeurism" (reviewing information not required by job duties) unless authorized to conduct such analyses. Examples include tracking the pattern of salary raises, viewing a colleague's personal information, looking up someone else's grades or viewing another colleague's work product when not authorized to do so.
- Circumventing the level of data access given to others by providing access that is broader than that available to them, unless authorized. For example, providing an extract file of employee salaries to someone who does not have security access to salary data is prohibited by this policy.
- Allowing unauthorized access to College's administrative systems or data by sharing an individual's username and password.
- Engaging in any other action that violates the letter and spirit of this policy, either purposefully or accidentally.

III Electronic Communication Policy

Purpose

Sri Sai Ram Institute of Technology has invested in its technology infrastructure to enhance teaching and learning and to enable efficient business practices. Student, faculty, and staff members have access to email, LMS and other apps as a communication tool for current news, events, personalized messages and teaching and learning activities. The College is committed to the use of College wide electronic communication to enhance interpersonal communications, improve information exchange, and to reduce the use of paper and printed materials.

The purpose of this policy is to identify electronic communication as an official means of communication within Sri Sai Ram Institute of Technology and to define the responsibilities of college students, faculty and staff related to electronic communication.

Statement of Policy

Sri Sai Ram Institute of Technology provides access to email /LMS for all faculty/ students and staff. Email is an official method of communication at College. Students, faculty and staff are held strictly responsible for the consequences of not reading College related communications sent to their official e-mail address.

Scope

Assigning of institutional email ID

Faculties and staff are assigned an email username and password upon acceptance to a program or upon hire. Core faculty, Coordinators and staff are assigned an additional username and password upon hire by the College, after being added to the Human Resource System. Core faculty will have both personal and Cells/committees email accounts. The official college email address is:

Faculty/Staff - username@sairamit.edu.in

Educational uses of electronic communications

Faculty members may require the use of email or other forms of electronic communication for course content delivery, class discussion, or synchronous chat. It is recommended that faculty specify these requirements in their course syllabus. Faculty may expect or require that students access LMS and college website to read notices sent to the official website, MIS and LMS.

Responsible use of email

Email, MIS and LMS are the tool provided by the College to complement traditional methods of communications and to improve education and administrative efficiency. All email users have a responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the college's e-mail system is confirmation that the user agrees to be bound by this policy. Violations of the policy may result in restriction of access to the College's email system and/or other appropriate disciplinary action.

The following should be observed when using any College email system:

- Conducting business for profit using College email and or other resources is prohibited. Incidental non-business personal use of e-mail is acceptable, but an expectation of privacy cannot be guaranteed due to the official nature of the email system;

- Using any email to send information that is classified as private or can be shown to contain personally identifiable information is prohibited. While the College will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through a College email system.

The following types of emails are explicitly prohibited:

- Emails that exchange proprietary information or other highly privileged, confidential or sensitive information.
- Emails that are considered advertisements, solicitations, chain letters, political communications and other unofficial, unsolicited email.
- Emails including sexual content, pornography, lewd or other highly inappropriate behavior when considering the official nature and purpose of the College email system.
- Emails that are in violation of any laws, including copyright laws, or Institutional policies.
- Emails that knowingly transmit a message containing a computer virus.
- Emails that intentionally misrepresent the identity of the sender of e-mail.
- Emails that use or attempt to use the accounts of others without their permission.

IV Personal Digital Assistant Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for the use and support of Personal Digital Assistant devices (PDAs) that are common in the workplace and may be used by employees of Sri Sai Ram Institute of Technology. This policy applies to, but is not limited to, all devices thatfit the following device classifications:

Handhelds running the Apple OS, Android OS, Blackberry OS, Palm OS, Microsoft Windows CE, PocketPC, Windows Mobile, Symbian, or Mobile Linux operating systems and others.

Mobile devices that are wireless or wired (i.e. connectible using the College wired or wireless network or by a wireless provider network such as Verizon, ATT or Sprint.

Smartphones that include PDA functionality.
Any third-party hardware, software, processes, or services used to provide connectivity to the above.

The policy applies to any PDA hardware and related software that could be used to access college resources, even if the equipment is not sanctioned, owned, or supplied by the college. The overriding goal of this policy is twofold.

The first goal is to protect the technology-based resources of the College (such as College data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attacks that could result in loss of information, damage to critical applications, loss of revenue or damage to our public image.

The second goal of this policy is to make clear the limits that the College places on user support for PDA devices.

V Wireless Network Policy

Purpose

Sri Sai Ram Institute of Technology provides wireless networking services in campus to enable the convenience of Internet connectivity. This service allows members of the College communityto access the campus wide network from wireless devices or portable computers where coverage is available.

The purpose of this policy and related procedures is to define responsibilities for the management and use of the wireless network and to manage other uses of the wireless spectrum and to ensure security across "Sri Sai Ram Institute of Technology" network.

Scope

The IT Department will regulate and manage all wireless access points used by wireless technology to ensure fair and efficient allocation and to minimize collision, interference, unauthorized intrusion and failure of the wireless network.

DEFINITIONS

Access Point (AP)

A hardware device that acts as a communication hub for users of a wireless device to connect to a wired network. APs are important for providing heightened wireless security and for extending the physical range of service to which a wireless user has access.

Wireless device

The end user system or device that accesses the wireless network for data communications purposes. This is normally a portable computer (Laptop) or personal digital assistant (PDA) containing an appropriate wireless network interface card (NIC).

PROCEDURES

Security

Users should assume that data transmitted over the wireless network is NOT secure.

Access Points

Only access points provided and installed by the IT Department or approved for installation by IT are permitted on the College network. IT reserves the right to disconnect and remove any access point not installed and configured by IT personnel or specifically covered by prior

written agreement and/or arrangement with IT. In cases where the device is being used for specific academic or research applications IT will work with faculty to determine how the wireless devices may be used while maintaining required security and without causing interference. Any person found responsible for the installation of unauthorized access points may be submitted to the appropriate college authority for disciplinary action. All access points shall be installed and configured in such a way as to comply with all security features of the wireless network, including restrictions to provide connections only to those users who are authorized to access "Sri Sai Ram Institute of Technology" network.

Other Wireless Devices

Unapproved wireless devices, such as portable phones and other devices with two-way radios may interfere with the operation of the College wireless network. If the IT department receives a report of interference and determines that a non-approved wireless device is causing interference with the College functioning, it reserves the right to ask the owner of the device to discontinue its use.

ALL THE ABOVE POLICY APPLIES TO:

This policy applies to all students, faculty, and staff of Sri Sai Ram Institute of Technology and to all other IT users of the "Sri Sai Ram Institute of Technology". These users are responsible for reading, understanding, and complying with this policy.

PRINCIPAL

Dr.K.PALANI KUMAR
PRINCIPAL
SRI SAIRAM INSTITUTE OF TECHNOLOGY
SAI LEO NAGAR, CHENNAI-600 044.