The South Indian Education Society
RISE WITH EDUCATION

Information Technology (IT) Policy
For Institutions under
The South Indian Education Society (SIES)

Prepared by

Manager-IT
Central IT Department, SIES

Reviewed by

Legal Advisor

Approved by

SIES Management

© 2025 The South Indian Education Society (SIES)
Confidential and not for public release. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—without prior written permission from SIES.

Document Version: 1.0
Dated: 22 April 2025

Index

Information Technology (IT) Policy for Institutions under The South Indian Education Society (SIES)

1. Introduction

This IT policy establishes guidelines for the ethical, secure, and efficient use of IT resources at SIES. It aims to enhance academic and administrative functions while ensuring data security, integrity, and responsible usage.

2. Purpose

The objectives of this policy are to:

- Define proper usage of IT resources.
- Maintain the security and integrity of IT infrastructure.
- Protect confidential institutional, student, and staff data.
- Prevent misuse and unethical activities related to technology.
- Promote responsible use of digital tools in academic and administrative settings.

3. Scope

This policy applies to:

- All students, faculty, staff, administrators and Advisors of SIES.
- All IT resources, including hardware (computers, digital devices, servers, networking devices, printers, scanners, etc.) and software (applications and systems).
- Communication platforms such as email, instant messaging, and social media.
- Internet access and external network usage.

4. Acceptable Use

- **Academic Use:** IT resources should primarily support education, research, and institutional communication.
- **Limited Personal Use:** Employees may use IT resources for personal purposes, provided it does not interfere with work responsibilities or violate policy guidelines.
- **Prohibited Activities:**
  - Accessing or sharing illegal, unethical, or inappropriate content.
  - Unauthorized commercial activities or personal financial gain.
  - Gaining unauthorized access to systems, data, or accounts.

- Engaging in hacking, cyber-attacks, or malicious activities.
- Installing unauthorized software on institutional devices.
- Sharing confidential information or violating privacy regulations.

5. Hardware Allocation & Management

- **Asset Assignment:**
    - Non-teaching staff will receive desktops/laptops based on work requirements.
    - Teaching staff should use shared computers in staff rooms or labs, except where a dedicated system is required.
    - Laptops are assigned only to employees requiring mobility for work duties.
    - Users must regularly log off or shut down their systems to ensure that Windows updates are installed properly, and system performance remains optimal. Failure to do so may result in missed updates, security vulnerabilities, or system instability.
- **One Employee, One Asset Policy:**
    - Employees are allocated a single IT asset (desktop or laptop).
    - The Head of Department (HoD) is responsible for departmental IT assets.
- **Asset Lifecycle:**
    - Devices will remain in use until they no longer meet operational needs.
    - Special hardware requests must include documentation justifying the requirement.
    - Asset must be returned to Central IT or institute IT team on resignation, retirement, termination, transfer to another institute or otherwise separation of services.
- **Employee Responsibilities:**
    - Employees must sign a declaration form upon receiving an IT asset and submit the same to the institute IT department, or Central IT, as the case may be.
    - Physical or other damage to device- will be repaired by SIES and costs recovered from employee. The employee shall not attempt any repair independently.
    - Upon resignation, , retirement, termination, transfer to another institute or otherwise separation of services. Devices, along with the accessories, must be returned in their original condition. While returning device and the accessories to the institute, employees should not delete any data from the system.

    - The use of unlicensed or unauthorized software is strictly prohibited, and any violation will result in disciplinary action.

6. Software Licensing Policy

- **Licensed Software Only**: All software installed on any PC or device or used within the **SIES Network** must be licensed. Only licensed software purchased by SIES shall be installed on the PC or device. The use of unlicensed or pirated software is strictly prohibited.

- Installation/Uninstallation of software/Operating system (e.g. Windows, Linux etc) should be done under only by Central IT/Institute IT department only.

- **Software Procurement**: All new software purchases must be processed through Central IT to ensure standardization, security, and compliance. A proper justification must be provided, and various available options must be evaluated before finalizing the purchase.

7. Agreement Requirement for Software Vendors

- **Mandatory Agreement:** Terms of the Agreement must be finalised with the software vendor before proceeding with any commercial discussions.
- **Legal Approval**: The Agreement must receive **approval from the Legal Head** to ensure compliance with organizational policies and legal requirements. Agreement will be signed by the authorised Managing Council member, and if required for statutory / compliance purposes, the HoI shall also be a joint signatory to this Agreement. Before starting any discussions with Vendors, confidentiality and NDA and no conflict-of-interest documents shall be signed by all persons involved in the negotiations and finalisation of terms.
- **No Commercial Discussions**: Until the Agreement is finalised, no financial or commercial negotiations should be concluded.

8. Access Management, Data Security & Privacy

- **Access Management:** Access to institutional IT systems, applications, and data is granted based on the principle of least privilege—users are given the minimum level of access necessary to perform their roles. All access rights must be authorized, documented, and periodically reviewed. User accounts are to be deactivated promptly upon role change, resignation, or completion of studies. Sharing of login credentials is strictly prohibited, and users are responsible for all activity performed under their accounts.

- **Data Protection:** All institutional data must be handled securely, with encryption and access controls in place.

- **Data Retention:** Data should be retained based on legal and regulatory requirements.

- **Access Control:** Users must not share credentials or grant unauthorized access to institutional data.
- **Password Management:** Strong passwords are mandatory, and multi-factor authentication (MFA) is encouraged.
- **OTP for Multi Factor Authentication (MFA):** Employees must not disclose the OTP received for multi-factor authentication (MFA) to anyone.
- **Data Backup:** Employees must regularly back up data to their respective OneDrive accounts to prevent data loss. Backup on personal Drives (like pen drive, external HDD or. online storage drive) is not allowed.
- **External Storage Devices:** The use of external drives is restricted, except for regulatory or government compliance purposes and the same must be approved by the HoI.
- **Data Handover:** Employees must ensure proper data handover upon resignation, , retirement, termination, transfer to another institute or otherwise separation of services, with responsibility lying with the immediate supervisor or Head of Institution (HoI).
- **Monitoring:** SIES regularly monitors usage of official email id, devices for any breach of guidelines mentioned in IT Policy.

9. Email & Login Guidelines

- **Email Creation/Deactivation:** Staff email IDs will be created or deactivated upon Central HR's request.
- Central HR Team shall email the Central IT team the details of the staff member/ Advisor whose email ids are required to be deactivated within 24 hours of the said staff member / Advisor services with ceasing to be associated with SIES for any reason.
- Student email ids will be created or deactivated upon the written request of the HoI.
- HoI shall email the Central IT/Institute IT team the details of the student whose email ids are required to be deactivated within 24 hours of the said student ceasing to be a student of SIES.
- All students should be made aware of the IT policy relating to students, and the same should be confirmed from the students in writing. A separate declaration form for the same will be made available.
- **Retention Approval**: A staff member's email ID can be retained only with approval from the **Head of Institution (HoI)** or **Central HR**. If an email ID is retained, the password will be **immediately changed** to ensure security and prevent unauthorized access.

- **Email Naming Convention:** Format: First name + first letter of last name; middle initial may be added if required.
- **Renaming of Email ID:** If an employee wishes to rename their email ID, the request must be routed through Central HR. Direct requests from employees will not be honoured.
- **Password Reset:** Students should contact their respective institute's IT department for email ID resets.
- **Official Communication:** Employees must use official email IDs for institutional communication.
- **Use of BCC (Blind Carbon Copy):** The use of BCC is discouraged as it may compromise the confidentiality and transparency of email communication. All recipients should be clearly visible to ensure accountability and promote open communication. If discretion is required, consider alternative, more secure methods of communication.
- **System Login:** Employees should log in using their official email IDs to ensure data backup to OneDrive.
- **Email & OneDrive Retention:** Employees must not delete email or OneDrive data upon resignation; violations will lead to disciplinary action.
- **Password Reset:** Currently, employees must contact respective IT support team or Central IT for password resets, but a self-reset system will be introduced.
- **Log off from system:** Employees must log out from their official email and OneDrive accounts after completing their work to ensure security and data protection.
- **Email Etiquette:** Users must maintain professionalism in email communications and refrain from sending spam, excessive attachments, or inappropriate and/ or offensive content.
- **Monitoring:** The institution reserves the right to monitor email traffic and other forms of communication for security and policy compliance.

10. Generic Email ID Creation & Disabling

- Institutes can raise a written request the creation of generic email IDs through the appropriate authority, providing a valid reason for the request and the person who would be accessing this email.
- To disable a generic email ID, Central IT requires written communication from the Head of Institution (HoI) or Registrar.

11. Bulk Email and SMS Communication

- The Bulk Email and SMS Service is provided for student and applicant communications. Central IT is the sole custodian of this service.
- Institutes must obtain approval from the management before utilizing this service.
- Central IT will provide necessary training to institutes on effective use of the service.
- Bulk Email Requests: Institutes wishing to send bulk emails should contact Central IT for assistance.

12. Distribution List Creation

- For the creation of employee and student email distribution lists, institutes must contact Central IT /Institute IT for activating/deactivating the same.

13. Microsoft Teams Usage Policy

- Since SIES has made a significant investment in Microsoft licensing, it is mandatory to use **Microsoft Teams** for all online meetings unless the non SIES connect does not want to use Microsoft Teams.

14. MS Teams Channel Usage

- **Official Communication:** Use **MS Teams channels** for team collaboration, discussions, and file sharing to maintain transparency and efficiency.
- **Channel Organization:** Create **separate channels** for different projects, departments, or topics to keep discussions focused.
- **Permissions & Access:** Ensure that only relevant team members have access to specific channels to maintain confidentiality and avoid clutter.
- **File Sharing:** Store and share documents within Teams to enable easy access and version control.
- **Meeting Integration:** Schedule and conduct meetings within Teams to streamline communication.

15. Student Email ID Management

- **Email ID Creation:** Student email IDs may be created in accordance with the institute's policy. These email IDs will be assigned under the sub-domain of **sies.edu.in** and can be created by the institute's IT administrator or Central IT.
- **Student Email Deactivation:** Student email accounts will be deactivated upon completion of their academic program. This measure is taken to maintain system security and ensure appropriate use of institutional resources. Students are advised to back up any important data prior to the completion of their course.If student fails or gets ATKT then in that case the email id remains active and it will be with student only.

16. Social Media Guidelines

- **Account Security:** Login credentials must be shared with Central IT, but the accountability related to the content that are being posted on social media rests with the individual who is responsible for it.
- **Verification:** Accounts should obtain verified status (blue tick) with management approval.

17. Website Management

- **Approval Process:** New website creation requires approval from Central IT and management.
- **Technical Standards for Web Development:** must avoid using vulnerable programming languages or obsolete technologies when creating or maintaining websites. The use of outdated or insecure technologies significantly increases the risk of hacking, malware, and ransomware attacks. All web development must adhere to current best practices in cybersecurity and use up to date, supported technologies.
- **Domain & Hosting:** Central IT will manage domain registration and hosting.
- **Content Guidelines:** Websites must contain accurate and up-to-date information while avoiding inappropriate, offensive or plagiarized content. No direct or indirect advertising, including surrogate advertising is allowed.
- **Collaboration:** Only if MoU or Agreement, which complies with the policy on MoUs or Agreements, is signed with the other entity. Similarly, use of SIES IPR is not allowed without prior written permission from the management.
- **Legal Compliance:** Websites must include disclaimers, terms of use, privacy policy, refund policy and copyright compliance.
- **Review Process:** Institutional leadership must approve website changes, and policies should be reviewed regularly. The website committee of each institute will be responsible for updating of respective website. Central IT will help in training the end user in case needed.

18. Internet/Network Usage

- **Internet Access:** Provided for academic and research purposes; personal use is discouraged.
- **Prohibited Downloads**: Downloading or installing games, unauthorized software, music, movies, or any other non-work-related or pirated content on institutional devices or networks is strictly prohibited. Such activities can expose systems to malware, legal liabilities, and bandwidth misuse. Only IT-approved software and content may be installed or accessed on institutional systems.
- **Security:** Users must not bypass institutional security protocols, and unauthorized device connections are prohibited.
- **Firewall Policy:** Each institute is equipped with a firewall to ensure the protection of user data and the integrity of the network. Users are strictly prohibited from disabling or bypassing the firewall under any circumstances. If there is an essential need to do so, it must be carried out strictly under the supervision and guidance of the Central IT team or the respective Institute IT team.
- **Malware Protection:** Antivirus software must be updated regularly, and users must not download or distribute malicious software, including worms, trojans.
- **Bandwidth Management:** Adequate bandwidth and backup connections are provided for uninterrupted access.

19. Software & Hardware Management

- **Software Licensing:** Only licensed software is permitted on institutional devices.
- **Device Usage:** Users must follow institutional guidelines for maintaining and securing devices.
- **Bring Your Own Device (BYOD):** If permitted, personal devices must comply with institutional security standards.

20.Online Forms:

- For creating online forms, it is advised to use Microsoft Forms only. If a Google Form is required, it must be created using an official Gmail ID. Central IT will assist in creating the official Gmail ID if needed. The details of the person authorised to access this Gmail id must be communicated in writing to the Central IT Team.

21. IT Support & Training

- **Support Services:** IT support is available for troubleshooting and technical training.
- **Training Programs:** Ongoing sessions will be conducted on technology usage, data security, and cybersecurity.
- **Incident response policy:** All users must immediately report any suspected or confirmed security incidents—including data breaches, malware infections, unauthorized access, or unusual system behaviour—to the Central IT Department or Institute IT team. The Central IT Dept/ IT team will initiate an incident response process that includes identification, containment, eradication, recovery, and post-incident analysis. Timely reporting is critical to minimize potential damage and maintain the integrity and security of institutional systems.

22. Cybersecurity Measures

- **Incident Reporting:** Security breaches must be reported immediately to the IT department.
- **Remote Software Usage Policy**
  The use of unauthorized remote access software such as Any Desk, Ultra Viewer, and TeamViewer is strictly prohibited. Only Microsoft Quick Assist is approved for remote support and troubleshooting. Ensure compliance with this policy to ensure security and prevent unauthorized access.
- **Training & Awareness:** Cybersecurity awareness programs will educate staff and students about phishing, malware, and security threats.
- **System Updates:** Security patches and updates must be updated as soon as the same is released.

23. Access to External Services

- **Cloud Services:** If cloud-based services (e.g., Google Drive, Microsoft Office 365) are used, institutional accounts should be used, and data stored on these services must be managed according to the institution's data privacy and security standards.
- **Third-party Applications:** Any third-party applications integrated with institutional systems must undergo a security review by the Central IT department to ensure they comply with data protection and security standards.

24. User Responsibility: Inadvertent and Intentional Acts

All users are expected to exercise due care when using institutional IT resources. Both inadvertent (accidental) and intentional actions that compromise system security, data integrity, or the confidentiality of information are subject to review and may result in disciplinary action. This includes, but is not limited to, accidental data leaks, unauthorized access, misuse of credentials, or intentional sabotage of systems. Users are encouraged to report any mistakes or incidents immediately to mitigate potential harm.

25. Consequences of Policy Violations

Non-compliance with this IT policy may result in disciplinary actions such as:

- Suspension of IT access.
- Disciplinary action Legal action, if applicable.

26. Policy Review & Updates

This policy will be periodically reviewed and updated in alignment with technological advancements, regulatory changes, and institutional requirements. All stakeholders will be informed of the updates once they are approved by the Management.

27. Advisory

Any non-compliance with the policy shall invite attendant consequences, including disciplinary action.

This is a broad framework of the institutional policies and protocols and is indicative and not exhaustive.

While care is taken to ensure that the IT systems function at optimal levels, there may be short term or long-term disruptions in the same, for reasons beyond the control of the IT team, including force majeure.