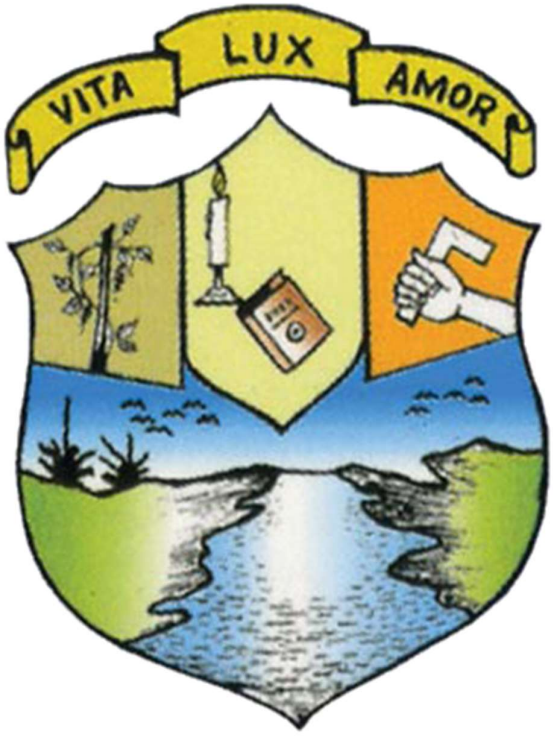
ST THOMAS COLLEGE PALAI
AUTONOMOUS | ESTD. 1950 | RE-ACCREDITED WITH A++ GRADE BY NAAC



ST. THOMAS COLLEGE, PALAI

INFORMATION TECHNOLOGY (IT) POLICY 2024

INFORMATION TECHNOLOGY (IT) POLICY

The College's Information Technology (IT) Policy, 2024 outlines guidelines for the responsible utilization of the college's IT resources. Recognizing the integral role of information technology in advancing the college's missions and administrative functions, as well as the imperative to safeguard information, this policy encompasses all centrally allocated or departmentally assigned IT facilities.

Applicable to faculty, staff, students, authorized visitors, and any other individuals utilizing college IT resources—whether personal or college-owned—this policy pertains to the accessing, transmitting, and storing of diverse forms of information. Users of the campus network and computer resources are entrusted with the proper utilization and safeguarding of these resources, while also respecting the rights of others.

The IT policy extends to resources managed by departments, including the Library, Computer Labs, Laboratories, and Administrative Offices. Additionally, it applies to computers owned by individuals, including research scholars and students, or research projects of faculty when connected to the campus network, subjecting them to the regulations outlined in the College IT Policy.

Objectives

- Uphold the maintenance, security, and lawful use of the college's information technology infrastructure within the campus premises.
- Deliver necessary IT resources to all stakeholders in accordance with academic standards outlined by regulatory bodies such as UGC, AICTE, and other relevant authorities.
- Develop comprehensive strategies and assign responsibilities across the college to safeguard accessed, created, managed, and controlled information assets.

- Guarantee the integrity, reliability, availability, and optimal performance of the college's IT systems.
- Serve as a guiding resource for stakeholders in utilizing the college's computing facilities, covering hardware, software, email, information resources, intranet, and internet access.
- Define and communicate directives on acceptable and prohibited actions, as well as procedures for addressing policy violations.

Guidelines for IT Hardware Installation and Maintenance

- System administrators are responsible for the installation and maintenance of IT hardware.
- Departments and faculties can submit their IT hardware requirements based on academic needs.
- Procurement of IT hardware is initiated based on stock availability and departmental requirements.
- The stock register is promptly updated upon procurement of IT hardware.
- Installation and maintenance services for IT hardware require approval from the department head and the principal.
- System administrators conduct periodic maintenance of computer systems, recorded in the maintenance register.
- Movement of IT hardware within or outside the college is documented in the Movement Register.
- Major e-waste items such as written-off instruments, CRTs, printers, computers, and batteries are regularly sold.
- Departments are accountable for the IT hardware provided to them, including any damage, loss, or theft.

Guidelines for Software Installation and Licensing

- The college IT policy permits the installation of authorized as well as the open-source software on college computers. Any violation of this policy will result in the department or individual being held personally accountable.
- Open-source software should be prioritized for use on college systems whenever feasible.
- Licensed software must be installed on college systems.
- Antivirus software must be obtained and installed on all college systems.
- System administrators are required to regularly backup data and store it on an external hard disk.
- Software utilized for academic and administrative purposes must adhere to ISO standards.

Guidelines for Network (Intranet and Internet) Usage

- The college is equipped with 200 Mbps of internet bandwidth provided by BSNL, enabling Wi-Fi connectivity across the entire campus for convenient access.
- Firewalls have been implemented to safeguard against cyber threats such as ransomware and unauthorized network access.
- All computers, including PCs and servers, connected to the college network must be assigned an IP address by the system administrators.
- Each allocated IP address is dedicated to a specific computer system and should not be shared with any other device, even if owned by the same individual and connected to the same port.
- Any alteration of IP addresses by staff or students is strictly prohibited.
- Network configurations are exclusively managed by system administrators.
- Departments or individuals intending to run server software over the LAN must first inform the system administrators.

- Connection to external networks via the college's network must adhere to the policies and regulations of those networks.
- Internet and Wi-Fi services are reserved solely for academic and administrative purposes.

Guidelines for E-mail Account Usage

- All faculty and administrative staff members are provided with individual institutional email IDs (G-Suite) and passwords.
- The primary purpose of these email accounts is for academic and official use, with limited allowance for personal correspondence.
- Any usage of the email facility for illegal or commercial activities is strictly prohibited according to the college's IT policy, and could result in the revocation of email privileges.
- Respecting privacy is paramount; users must refrain from attempting to access or intercept other users' email accounts.
- Impersonating the email accounts of others is considered a severe breach of the college's IT security policy.
- All email correspondence must align with institutional and ethical guidelines, ensuring it remains free from offensive or controversial content in both creation and distribution.
- Ultimately, it is the responsibility of each individual to maintain their email account in compliance with the college's email usage policy.

Guidelines for Website Hosting

- The College Website Updation Committee is tasked with ensuring the accuracy and clarity of academic and administrative information provided on the college website. This includes updating and maintaining content, proofreading pages, and rigorously testing links before publication.

- All information hosted on the website must be correct and easily comprehensible to its stakeholders.
- Moreover, the website may integrate data directly sourced from the college's ERP software to enhance efficiency and accuracy.
- It will also serve as a hub for accessing admission procedures and other administrative services within the college.
- Departments and their respective associations, as well as events organized by them, may have dedicated web pages. These pages must adhere to the College Web Site Creation Guidelines to maintain consistency and professionalism across the website.
- Additionally, integration with the Learning Management System (LMS) allows faculty to share class materials online, facilitating eLearning for students.
- The Website Update Committee must prioritize data security measures to safeguard all hosted information effectively.

Guidelines for College Database Utilization

- The college administration maintains databases crucial for e-Governance, necessitating robust protection measures. As the data owner, the college holds all institutional data generated within its premises. Various individuals or departments contribute segments to these databases and may have custodial duties over specific data portions.
- The college's data policies strictly prohibit the dissemination of personally identifiable data to external entities. Information collected, whether by departments or individual faculty/staff, is strictly for internal use within the college community. Access to data aligns with one's role and responsibilities, as defined by the college's data access policies.

- Under no circumstances should data directly identifying individuals or their personal information be shared with external parties, including government agencies, surveys, or other requests. Such requests are to be directed to the college's IQAC Office.
- Requests for information from legal entities like courts or law enforcement agencies are managed centrally by the college's Office, and departments should refrain from responding independently. Additionally, releasing information, including 'Directory Information', for commercial or solicitation purposes is strictly prohibited.
- Preparation and submission of reports for government agencies like UGC or KSHEC are the responsibility of designated college officials, supervised by the principal, vice principal or IQAC coordinator.
- Tampering with the database, including unauthorized alterations by departments or individual users, constitutes a violation of the college's IT policy. Such actions may result in disciplinary measures by the college authorities, and in cases of illegal activity, law enforcement may be involved.
- All intranet applications operate on web servers owned by the college.

Guidelines for Video Surveillance

- Surveillance cameras are widespread across various locations within the campus, with regular monitoring of video footage.
- Access to the control room is strictly prohibited without authorization.
- Footage retrieval requires prior approval from the principal.
- Routine maintenance ensures camera functionality.
- Live monitoring is conducted by the authorities, including the principal, vice principal, bursar, and administrative head.

Responsibilities of Network/ System Administrators

- Designing and overseeing the college network infrastructure, adhering to global naming and IP address standards.
- Evaluating current networking resources and determining expansion needs.
- Configuring and managing both wireless and local area networks.
- Maintaining IT equipment in classrooms, labs, seminars, and workshops. Addressing user complaints regarding network issues.
- Managing servers in the server room.
- Overseeing maintenance of computer hardware, peripherals, and networking devices.
- Enforcing policies against unauthorized software installation on user systems, refraining from accommodating such requests.

Guidelines for E-waste Management

The college has implemented various e-waste management initiatives with the aim of fostering an eco-friendly environment across campus.

E-Waste Management Practices

- Electronic devices undergo thorough assessment for potential reuse; minor issues are resolved by laboratory assistants and teaching staff, while major repairs are handled by technical personnel before being reintroduced into circulation.
- E-waste such as obsolete instruments, CRTs, printers, and computers are sold off.
- UPS batteries are either recharged, repaired, or exchanged through suppliers.
- Regularly depreciated electronic gadgets, circuits, and kits are sold to interested buyers.

- Miscellaneous e-waste items including CDs, batteries, fluorescent bulbs, and PCBs are systematically collected from all departments and offices for proper disposal.
- Waste CDs and other non-hazardous disposable items are repurposed by students for decorative purposes.
- Awareness Initiatives: Educational programs are conducted within the college to educate students about effective e-waste management techniques.

IT Usage and Prohibitions

- The users within the college community are expected to utilize various campus resources effectively, including but not limited to collaboration systems, internet connectivity, wireless networks, official websites (such as the college website, conference portals, journal platforms, online admission systems, and course-specific sites), management information systems (MIS) and ERP solutions, learning management platforms, and electronic library materials.
- Emphasis is placed on compliance with college policies and legal requirements, encompassing licenses and contractual obligations.
- Prohibited activities include sending, accessing, or downloading materials that are fraudulent, harassing, obscene, threatening, or otherwise infringe upon applicable laws or college regulations. Creating an environment that fosters hostility within academic or professional settings is strictly forbidden.
- Respect for copyrights and adherence to licensing agreements concerning copyrighted content is paramount. Engaging in unlawful file sharing using college resources constitutes a violation of policy.
- Users are expected to adhere to college guidelines concerning the use of social media platforms, mailing lists, news outlets, chat rooms, and blogs.

- Commercial exploitation of college IT resources, including promotional activities through advertisements or solicitations, is prohibited unless explicitly permitted by college regulations.
- Personal use of college IT resources should not compromise the institution's core functions or mission, except when such activities are purely incidental.
- Unauthorized access to information is strictly prohibited, with an emphasis on promoting secure network and computer access protocols.
- To bolster cybersecurity measures, procedures for managing internet and intranet traffic flow are enforced through unified threat management, including firewall protocols.
- Regular updates to antivirus software and security protocols are essential to safeguarding computing resources against potential threats.

Operating Aspects

- The College is committed to equitably implementing this policy in alignment with its foundational goals. The management of operational IT resources shall adhere to the hierarchical structure of college governance.
- It is the duty of the heads of respective institutions to ensure compliance with all college policies regarding the utilization and ownership of information resources, while remaining mindful of the college's vision and mission.
- The users are solely responsible for the activities they perform on College servers with their "User Name/Password" pairs and IP (Internet Protocol) addresses assigned to them.
- The college-level website and technical committee will collaborate on various activities concerning compliance with the IT policy, in conjunction with the college's IT administrator.

Maintenance

Users can register complaints via https://mro.stcp.ac.in/stcp. The IT Division accepts complaints from users regarding any issues with computer systems or peripherals under maintenance through them. The Network Administrator in the IT Division manages complaints from users and collaborates with service engineers of the respective brands (under warranty) to resolve the issues within a reasonable timeframe.

Termination of User Account

User accounts on the St. Thomas College network systems and other IT resources may be terminated or disabled, with or without prior notice, for various reasons, including inappropriate use of computing and network resources. Faculty and staff accounts will be terminated upon retirement or cessation of official responsibilities on campus, while student accounts will be terminated upon completion of their courses.

Violation of Policy

Any breach of the fundamental objectives and areas outlined in the college's IT policy will be deemed a violation and constitute gross misconduct under the college regulations. The college will periodically determine the requisite rules for implementing this policy.

Review and Monitoring

The policy document should undergo a thorough review every two years to ensure its alignment with the evolving landscape of IT-related developments in the industry. If necessary, updates should be made to reflect these advancements.

The "IT Policy, 2024" of the college, underscores the importance of responsible utilization and safeguarding of IT resources. It ensures alignment with the institution's missions and administrative functions while prioritizing

information security. Through compliance with regulations, including those pertaining to department-managed resources and individual-owned computers connected to the campus network, the policy upholds the integrity and security of college IT infrastructure.