MANNAR THIRUMALAI NAICKER COLLEGE

(Founded by the Tamilnadu Naidu Mahajana Sangam)

An Autonomous Institution, Affiliated to Madurai Kamaraj University

A Linguistic Minority Co-educational Institution/ Re-accredited with 'A' Grade by NAAC

PASUMALAI, MADURAI – 625 004

IT POLICY

IT Policy

Mannar Thirumalai Naicker College is committed to providing a secure, efficient, and responsible information technology (IT) environment for the benefit of its students, faculty members, staff members, and administration. This IT policy document serves as a guide to ensure the appropriate and ethical use of IT resources within the College. The policies outlined herein are designed to safeguard data, protect networks and promote the responsible and efficient use of technology.

The IT policy applies to all individuals who access, use, or manage IT resources provided by the college, including computers, networks, internet access, software, and electronic communication systems. It is essential that all members of the College are aware of and adhere to these policies to maintain a sccurc and productivc IT cnvironmcnt.

The Purpose of the IT policy:

1. Define acceptable and prohibited use of IT resources
2. Ensure network and information security
3. Manage software installation and licensing
4. Govern hardware installation and Maintenance
5. Promote Email and communication best practices
6. Manage and support the implementation, maintenance and optimization of the organization's ERP system.
7. Initiate the procurement process for IT-related purchases.
8. Establish and enforce regulations for the utilization of Wi-Fi connectivity within the campus.
9. Ensure the protection of confidential office data.
10. The allocation of IP addresses and authentication process is through the firewall.
11. The management of the official website of the College
12. Describe the IT-related roles and responsibilities

Management Information Cell (MIC)

The resolution of the day-to-day IT issues by the System Administrators in consultation with the MIS Convener. However, the MIS Cell, comprising the following members, is accountable for making major policy decisions and implementing changes related to the IT resources of the College

1. Principal (Chairperson)
2. Honourable Secretary
3. College Coordinator – IQAC
4. Convener & Co-convener – MIS
5. Head of the Department of Computer Science
6. System Administrator
7. Hardware Technicians

Definition of Acceptable and Prohibited Use of IT resources

The IT resources provided by the Institution, including internet connectivity and official email accounts, as well as computer systems for the staff and the students, are intended solely for official and educational purposes. The College reserves the right to monitor internet usage by staff members if the need arises. Hence, the staff and the students are not expected to use these resources for personal work. Additionally, the college insists that all users of the College network comply with the IT laws of the country.

Ensure Network and Information Security

- Do not attempt to access systems, files, or resources for which you do not have proper authorization. Unauthorized access is a violation of IT policies and can result in disciplinary actions.
- Avoid sharing your login credentials, such as usernames and passwords, with others. Each individual should have their own unique login information for accountability and security purposes.
- Refrain from downloading and installing software on College computers or devices without proper authorization. Unauthorized

software can introduce security risks and may violate licensing agreements.

- Do not use the College network or IT resources for cyberbullying, harassment or any other form of malicious behavior towards others. Respectful and courteous communication is essential.
- Be cautious of suspicious emails or messages that ask for personal information or login credentials. Do not click on unknown links or download attachments from untrusted sources.
- Avoid connecting malware-infected devices to the College network, as they can compromise the security of other devices on the network.
- Do not connect unauthorized network devices, such as routers or access points, to the college network without proper authorization. These can create security vulnerabilities.
- Adhere to the college's network usage policies, which may include limitations on bandwidth usage, streaming, or accessing certain websites.
- Do not neglect software updates and security patches on personal devices connected to the college network. Keeping devices up to date helps prevent security vulnerabilities.
- Avoid attempting to bypass security measures, such as firewalls or access controls, to gain unauthorized access to resources.

By following these "don'ts" and being mindful of responsible IT practices, all users can contribute to a safer and more secure College network environment for everyone.

Manage Software Installation and Licensing

The management of software licensing-related activities of the College falls under the responsibility of the MIS cell. The System Administrator is accountable for preventing any form of software piracy and other IT-related crimes within any section of the College. The College is dedicated to using exclusively licensed versions of software. To avoid potential licensing-related

complications, the College encourages the adoption of open-source software and operating systems.

Govern Hardware Installation and Maintenance

To ensure systematic and effective hardware maintenance and optimal utilization of available IT resources, the hardware technicians implement the following initiatives:

Authorization for Repairs: Only hardware engineers are allowed to conduct repairs or replace parts, ensuring proper and responsible usage of IT resources.

Stocking Essential Peripherals: At the start of each academic year, essential peripherals and parts are purchased and kept in stock, expediting the repair process when needed.

System Inspection by Hardware Engineers: Hardware Engineers take responsibility for inspecting computer systems to identify possible errors and performance issues.

UPS Connection for Computers: All computers and peripherals are connected to electrical points via UPS systems with proper earthing and wiring to safeguard against power fluctuations and outages.

Network Cable Placement: Network cables are kept away from electrical and electronic equipment to prevent interference and maintain network stability.

Timely Equipment Replacement: ICT equipment is replaced only when necessary or uneconomical to repair, ensuring cost-effectiveness and optimal utilization of resources.

Maintenance Complaint Handling: The designated team is responsible for handling maintenance-related complaints concerning centrally purchased computers distributed by the MIS.

By adhering to these measures, the Hardware Technicians maintain hardware effectively and ensure the smooth functioning of the IT

infrastructure of the College while promoting responsible resource management.

Promote Email and Communication practices

- The College provides institutional email addresses to all the faculty members and students, which should be used for all official and college-related activities and communications.
- For students, the email addresses allotted during their programmme of study will be discontinued three months after completing their programme. However, students joining higher studies within the College will be provided with separate email addresses.

Manage and Support the Implementation, Maintenance, and Optimization of the Organization's ERP system.

- Organize training sessions for the staff members and the faculty to familiarize them with the centralized campus management system. Provide ongoing support and assistance to users, addressing their queries and resolving any issues that may arise.
- Regularly gather feedback from users and stakeholders to identify areas for improvement in the functioning of the systems. Work with the vendor or development team to implement enhancements and updates as needed.

Initiate the Procurement Process for IT-related Purchases

- Prior permission from the honourable College secretary and the Principal is required for all IT-related purchases.
- For all bulk purchases, three quotations are collected and submitted to the Management. The Purchase Committee of the Management then makes the decision based on the requirement.

Establish and Enforce Regulations for the Utilization of Wi-Fi Connectivity within the Campus

- Before connecting any new device to the College network, individuals must seek permission from the MIS Convener.

- To manage the use of WIFI connectivity on campus, all WIFI users are identified and assigned unique IP addresses.
- Students and staff members wishing to access the college internet on their personal devices must submit an application in the prescribed format, available from the system administrator, with the principal's approval.

Allocation of IP Addresses and Authentication Process

In order to regulate WIFI internet access on the campus, users are required to authenticate through IP allocation and the firewall. Additionally, certain websites are blocked to prevent misuse of the college internet. The system administrator, with the MIS Convenor's approval, maintains and refreshes the list of restricted websites on a yearly basis.

The Management of the College Official Website

The responsibility for managing the official website lies with the Website Administrator. The Website Administrator is tasked with ensuring regular updates to the website. Changes to static components are expected to be implemented within 24 hours, while dynamic components should be addressed on the same day, within 12 hours.

Describe the IT-related roles and responsibilities

Roles and Responsibilities for Lab Technicians

- Assist in setting up and arranging computer hardware, peripherals and other lab equipment
- Ensure that all computers are clean, functional and properly connected to power and network resources
- Assist lab users in accessing and utilizing lab resources effectively and efficiently
- Educate lab users about the best practices for data security, safe internet browsing, and responsible computer usage
- Enforce lab rules and policies regarding appropriate lab conduct, resource usage and access control

- Collaborate with the faculty members and the support staff to assist academic activities and ensure supply of lab resources meet educational requirements
- Ensure the lab environment is safe and compliant with health and safety regulations
- Familiarize lab users with safety protocols and provide guidance on proper equipment handling to prevent accidents
- Maintain attendance records and logbooks for lab users, as required
- Assist in managing lab schedules, reservations and coordinating access for special events or classes.

Roles and Responsibilities for Hardware Technicians

- Maintain an organized and clutter-free lab environment by arranging cables and keeping workstations tidy.
- Troubleshoot and resolve technical issues related to computer hardware, peripherals, and software.
- Provide training or orientation sessions to new lab users on lab guidelines, equipment usage and available resources.
- Conduct regular inspections to identify and address potential hazards in the lab
- Regularly clean lab workstations, keyboards, mice and other peripherals to maintain hygiene.

Roles and Responsibilities for System Administrator

- Perform regular inspections and preventive maintenance to ensure proper functioning of equipment.
- Install and configure necessary software and updates on lab Computers.
- Keep an inventory of lab equipment and coordinate with procurement for repairs or replacements as needed.
- Provide technical guidance and support for software installations, configurations and usage.

- Help Lab Technicians to troubleshoot computer and software issues and escalate complex problems to appropriate support channels, if necessary.
- Address user inquiries, questions, and requests regarding lab operations and policies.
- Provide guidance on data backup, storage, and file management practices for lab users.
- Implement and maintain security measures to protect lab computers and network infrastructure.
- Participate in the development and revision of lab policies and procedures in collaboration with lab administrators and relevant stakeholders.
- Monitor and report any security breaches or suspicious activities within the lab.

Roles and Responsibilities for Network Analyst

- Design, implement, and maintain the college network infrastructure.
- Monitor and ensure network connectivity, availability, and performance.
- Administer network devices such as routers, switches, firewalls, and wireless access points.
- Configure and manage network security measures, including firewalls, intrusion detection/prevention systems, and VPNs
- Manage user accounts, permissions, and access control for network resources.
- Monitor network traffic, identify potential security threats and implement appropriate measures for network protection
- Troubleshoot network issues, diagnose and resolve network outrages and perform root cause analysis.
- Perform regular network backups and ensure data integrity and disaster recovery.
- Provide technical guidance and support to users and colleagues on network-related matters.

- Conduct network audits and assessments to identify vulnerabilities and propose improvements.
- Document network configurations, changes and procedures for future reference.
- Maintain relationships with vendors and service providers for network-related procurement and support.

The above IT policy encompasses the following stakeholders:

- Students
- Faculty Members
- Administrative Staff
- Higher Authorities and Officers
- Guests

MANNAR THIRUMALAI NAICKER COLLEGE (AUTONOMOUS) PASUMALAI MADURAI 625 004

PRINCIPAL
MANNAR THIRUMALAI NAICKER COLLEGE
(AUTONOMOUS)
PASUMALAI, MADURAI-625 004