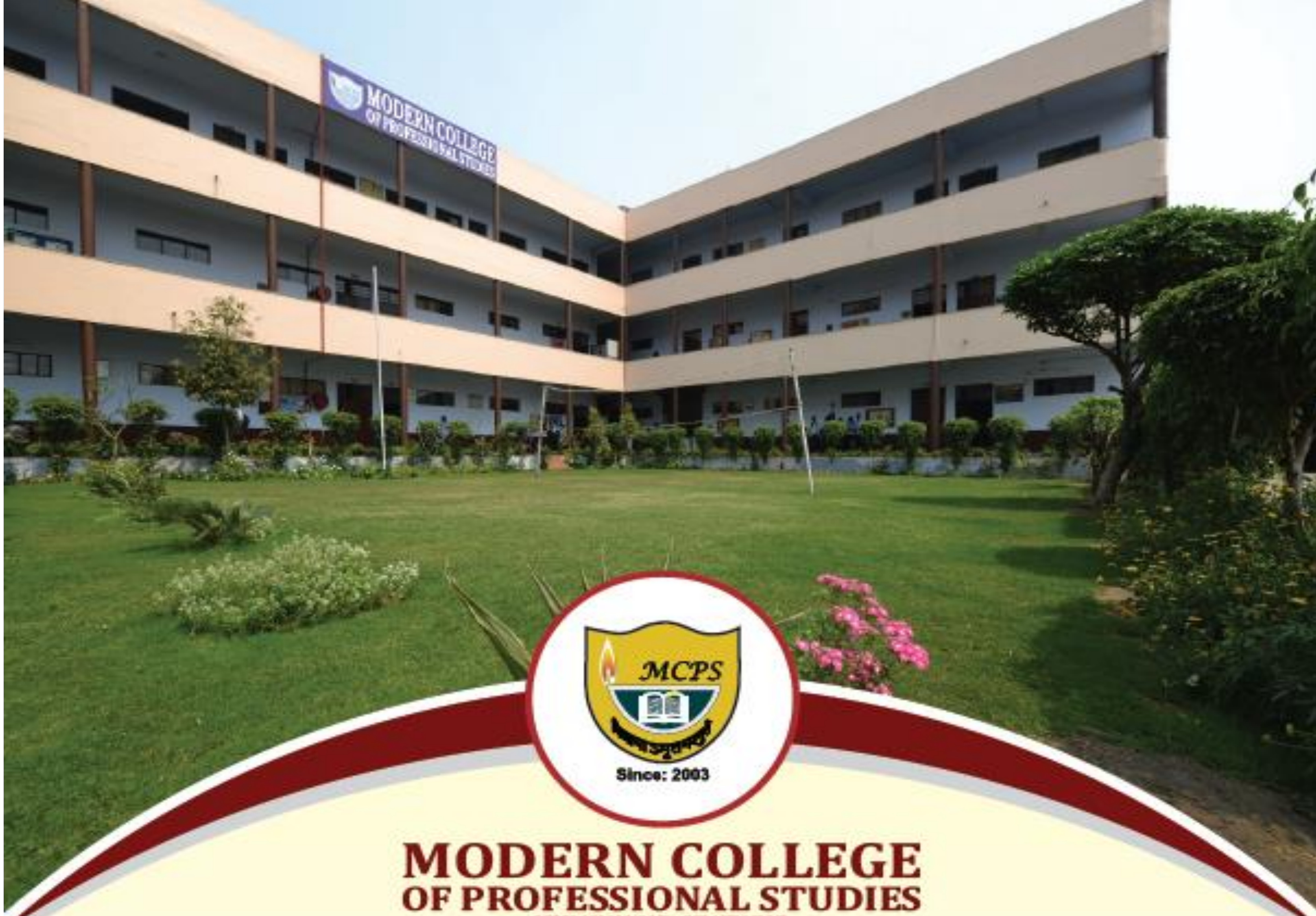

# MODERN COLLEGE OF PROFESSIONAL STUDIES

MOHAN NAGAR, GHAZIABAD

*(Affiliated to CCS University, Meerut )*

# Information Technology Policy (2023)

## Preamble

In today's digital age, information technology (IT) is integral to the academic and administrative functions of Modern College of Professional Studies. The college recognizes the importance of reliable and secure IT resources for enhancing educational experiences and operational efficiency. This policy aims to establish guidelines for the responsible use of these resources, aligning with the college's mission and values while fostering an environment conducive to learning, teaching, research, and administration.

## Purpose

The purpose of this policy is to provide a framework for the acceptable use of IT resources at Modern College of Professional Studies. The policy outlines the guidelines for the responsible use of these resources, protecting their integrity, reliability, and availability. Additionally, it seeks to promote ethical and responsible use of IT resources while ensuring compliance with legal and regulatory requirements.

## Objectives

- Define the boundaries of acceptable use of IT resources.
- Safeguard the college's data and systems from potential threats.
- Encourage the use of IT resources for educational and administrative purposes.
- Prevent misuse of IT resources.

## Scope

- Students, faculty, and staff.
- Contractors, vendors, and visitors.
- College-owned and personal devices connected to the college's network.

## IT Cell / Committee

❖ The college will establish an IT Cell or Committee responsible for:

- Overseeing IT operations and resources.
- Developing and implementing IT policies and procedures.
- Monitoring and addressing IT issues and incidents.
- Providing guidance and support on IT-related matters.

❖ The IT Cell or Committee will consist of:

- An IT Head or Coordinator.
- Faculty and staff members with relevant expertise.
- Student representatives, if applicable.

## Functions of the IT Cell / Committee

❖ The functions of the IT Cell or Committee will include:

- Policy Management: Developing, reviewing, and updating IT policies and procedures.
- Security Management: Monitoring IT security and addressing breaches or incidents.
- Resource Management: Overseeing IT resources and infrastructure, including hardware, software, and networks.
- User Support: Providing technical support and training to users.
- Compliance Management: Ensuring compliance with legal and regulatory requirements.

## Use of IT Resources

- ❖ Acceptable Use: IT resources must be used for educational and administrative purposes, such as:
  - Teaching, learning, and research.
  - Administrative operations and communication.

- ❖ Unacceptable Use: IT resources must not be used for the following:
  - Illegal Activities: Using IT resources for illegal activities, such as hacking, unauthorized access, or spreading viruses or malware.
  - Inappropriate Content: Accessing or sharing obscene, offensive, or discriminatory content, including pornography, hate speech, or defamatory or libellous content.
  - Misuse: Using IT resources for personal gain, political campaigning, or commercial advertising, including running a private business or sending political messages or spam.
  - Intellectual Property Infringement: Using IT resources in violation of intellectual property rights, such as sharing copyrighted materials without permission**.**

## Security

- ❖ Users must not share their passwords or access codes. Passwords should be:
  - Unique and not easily guessed.
  - Changed regularly and kept confidential.

- ❖ Users must report any security breaches or suspicious activities to the IT Cell or Committee, such as:
  - Unauthorized access to accounts or systems.
  - Malware infections or phishing attempts.

- ❖ The IT Cell or Committee will:
  - Monitor the network for security threats.
  - Implement security measures to protect IT resources.
  - Respond to security incidents and breaches**.**

## Data Backup and Recovery

The IT System In charge is responsible for periodically backing up the college's ERP, website, and other data. Additionally, the Web Administrator is expected to conduct security audits on IT systems in different sections of the college, in consultation with the principal, using the available resources to identify possible security issues and threats.

## Use of Wi-Fi

- Permission must be obtained from the IT System head before connecting any new device to the college network.
- To regulate the use of Wi-Fi connectivity in the college campus, all users of Wi-Fi are recognized and allotted unique IPs.

## Confidentiality and Privacy of Official Data

- Members of the college community who have access to the college database and personal details of students must respect the privacy of students and maintain confidentiality when dealing with student details.
- The college does not share the student database with anyone, even for campus placement drives. However, details of students who have signed up for a placement drive may be shared with the concerned firm, with a request to respect student privacy.
- The college does not spam students' mailboxes with promotional content.

## Electronic Communication Systems

- The institutional email ID must be used for all official communications.
- Since the electronic communication systems are the property of the institution, all members must abide by the institutional code of conduct for diligent use.
- The institution has the right to delete, amend, or modify any communication detrimental to its rights.

## Software Licensing and Hardware Maintenance

- The IT administration committee must approve software installations on campus.
- The software must be used by committee members for authorized purposes only.
- Third-party software must be procured with the necessary licenses registered in the name of the institution.
- Pirated software is strongly discouraged by the committee.
- Appropriate antivirus software will be installed on all computers, laptops, and devices accessed by the college.
- Trained IT staff, selected by committee members, will be responsible for identifying and resolving issues.
- All computing and networking devices shall be purchased from authorized vendors through legal tenders.

## Disciplinary Actions

- ❖ Violations of this policy may result in disciplinary action, including:
  - Suspension or termination of IT access.
  - Disciplinary action by the college administration.
- ❖ Violations may also result in legal action, including:
  - Civil or criminal penalties.
  - Reporting to law enforcement authorities.

## Policy Review

This policy will be reviewed annually and updated as necessary by the IT Cell or Committee in consultation with the college administration. The review will assess the effectiveness of the policy, address changes in technology or regulations, and incorporate feedback from users or stakeholders.

NISHA SINGH

Digitally signed by NISHA SINGH
Date: 2024.08.29 16:41:49 +05'30'