मा.मारुतरावजी घुले पाटील कला, वाणिज्य व शास्त्र महाविद्यालय
अहमदनगर
बहुजन हिताय । बहुजन सुखाय ॥

IT(information Technology) POLICY

IQAC Department

Janata Shikhan Prasarak Mandal’s

Marturaoji Ghule Patil Art’s,Commece And Science College

Ahmednagar Maharashtra India 414111

IT(Information Technology) POLICY

Policy Statement:

The Information Technology (IT) Policy of Marutraoji Ghule Patil College, Ahmednagar outlines the guidelines, rules, and responsibilities related to the use of information technology resources within the college. This policy aims to provide a secure, reliable, and efficient IT environment that supports the college's mission and goals.

Information technology plays a crucial role in facilitating teaching, learning, research, administrative processes, and communication within the college community. It is vital for supporting academic programs, enhancing operational efficiency, and fostering innovation. The IT Policy acknowledges the significance of information technology as a strategic asset and commits to its effective utilization.

The primary objective of this policy is to ensure the availability, integrity, and confidentiality of the college's IT resources. It emphasizes the need for responsible and ethical use of technology, promoting a culture of security awareness, and compliance with relevant laws, regulations, and policies.

The IT Policy covers a wide range of IT aspects, including acceptable IT devices, user responsibilities, data network management, computing facility provisioning, software management, network connectivity, security measures, network services, prohibited activities, and consequences of policy violations.

To achieve a secure and efficient IT environment, the college will implement appropriate technical measures, security controls, and monitoring mechanisms. Regular updates, training programs, and awareness campaigns will be conducted to educate users about IT policies, best practices, and emerging threats.

The IT Policy applies to all faculty, staff, students, and any individuals granted access to the college's IT resources. Compliance with this policy is mandatory, and violations may result in disciplinary actions, including but not limited to, loss of IT privileges, academic penalties, or legal consequences.

By implementing this IT Policy, Marutraoji Ghule Patil College demonstrates its commitment to providing a robust and reliable IT infrastructure that supports the college community's academic and administrative activities. This policy sets the foundation for responsible IT usage, data security, and efficient IT operations, fostering a culture of innovation, collaboration, and continuous improvement within the college.

Objectives:

The IT policy of Marutraoji Ghule Patil College is designed to achieve several key objectives. These objectives guide the development, implementation, and enforcement of the policy to ensure the efficient and secure use of information technology resources. The main objectives of the IT policy are as follows:

1. Availability and Reliability of IT Resources:

- Ensure the availability of IT resources, including network services, computing facilities, software, and data, to support the academic and administrative functions of the college.

- Implement measures to enhance the reliability, performance, and resilience of IT infrastructure, minimizing downtime and disruptions.

2. Security and Protection of Sensitive Information:

- Establish and maintain robust security measures to protect the confidentiality, integrity, and availability of sensitive information, including personal data, research data, financial records, and intellectual property.

- Implement access controls, encryption, authentication mechanisms, and other security measures to safeguard against unauthorized access, data breaches, and malicious activities.

3. Responsible IT Usage:

- Promote responsible and ethical use of IT resources by all members of the college community, including faculty, staff, and students.

- Educate users about their responsibilities, acceptable use policies, and best practices to ensure appropriate and lawful utilization of IT resources.

- Raise awareness about cybersecurity risks, social engineering, phishing attacks, and other potential threats, and provide training and resources to help users protect themselves and the college's IT environment.

4. Compliance with Laws and Regulations:

- Ensure compliance with applicable laws, regulations, and industry standards governing information security, data protection, copyright, intellectual property, and other IT-related legal requirements.
- Stay updated with emerging laws and regulations related to information technology and incorporate necessary changes into the policy to maintain legal compliance.

5. IT Governance and Accountability:

- Establish clear roles, responsibilities, and accountability for IT governance within the college.
- Define processes for decision-making, prioritization, resource allocation, and oversight of IT-related initiatives, ensuring alignment with the college's strategic goals and objectives.
- Foster a culture of accountability, where users understand their responsibilities and are aware of the consequences of policy violations.

6. Continual Improvement:

- Regularly review and update the IT policy to incorporate changes in technology, best practices, and evolving security threats.
- Seek feedback from the college community to identify areas of improvement and address emerging challenges and concerns related to IT usage.
- Encourage innovation and explore opportunities to leverage technology for enhancing teaching, learning, research, and administrative processes.

By aligning with these objectives, Marutraoji Ghule Patil College aims to create a secure, reliable, and efficient IT environment that supports the college's mission, enhances productivity, fosters innovation, and protects the interests of its stakeholders.

I) Acceptable IT Devices:

Marutraoji Ghule Patil College permits the use of various IT devices to support the academic and administrative functions of the institution. This section specifies the types of IT devices that are acceptable for use within the college and provides guidelines on their appropriate usage. Additionally, guidelines for the use of personal devices on the college network and any restrictions or requirements for using college-provided IT devices are outlined.

1. Acceptable IT Devices:

The following IT devices are considered acceptable for use within the college, subject to compliance with the IT policy and guidelines:

- Desktop computers
- Laptop computers
- Tablets
- Smartphones
- Printers and scanners
- Projectors and audiovisual equipment
- Network switches and routers (for authorized IT personnel)
- Other devices approved by the college's IT department or administration for specific purposes.

2. Guidelines for Personal Devices:

- Personal devices, such as laptops, tablets, and smartphones, may be used on the college network, provided they comply with the acceptable use policy and adhere to the following guidelines:

a. Personal devices should be kept updated with the latest operating system patches and security updates to ensure they do not pose a risk to the network or other devices.

b. Users are responsible for securing their personal devices with strong passwords or other appropriate authentication methods.

c. Personal devices should not interfere with the network's performance or disrupt the activities of other users.

d. Users should refrain from downloading or installing unauthorized software that may compromise the security or integrity of the network.

3. College-Provided IT Devices:

- College-provided IT devices, such as laptops, tablets, or other equipment, may be issued to faculty, staff, or students for specific purposes.

- Users of college-provided IT devices are expected to adhere to the following requirements and restrictions:

a. Users should use college-provided IT devices solely for authorized purposes related to their academic or administrative responsibilities.

b. College-provided IT devices should be used in accordance with the IT policy and guidelines, including restrictions on unauthorized software installation, prohibited activities, and data protection requirements.

c. Users should take appropriate care of college-provided IT devices, ensuring they are not lost, stolen, or damaged.

d. Users must report any loss, theft, or damage to college-provided IT devices promptly to the IT department or designated authority.

It is important for users to understand and comply with the guidelines for acceptable IT devices. By using IT devices responsibly and adhering to the policy, users contribute to a secure and reliable IT environment within Marutraoji Ghule Patil College.

II) Responsibilities of Users and User Groups:

At Marutraoji Ghule Patil College, all users, including faculty, staff, and students, have specific responsibilities regarding IT usage. Adherence to these responsibilities is crucial to maintain a secure and efficient IT environment. The following guidelines outline the key responsibilities for each user group:

1. Faculty:

- Use IT resources to enhance teaching, research, and administrative tasks in accordance with college policies and academic goals.
- Protect and secure sensitive data related to research, student records, and intellectual property.
- Encourage students to follow IT policies and guidelines.
- Report any IT issues or security incidents promptly.
- Maintain the confidentiality and integrity of student data in accordance with privacy regulations.

2. Staff:

- Use IT resources for official college activities and administrative purposes only.
- Safeguard confidential and sensitive information.

- Adhere to password security guidelines by using strong passwords, avoiding password sharing, and changing passwords periodically.

- Report any suspected security breaches or IT issues to the appropriate IT support channels.

- Follow acceptable use policies and guidelines for internet, email, and software usage.

3. Students:

- Use IT resources for educational purposes and college-related activities.

- Protect their login credentials and use strong passwords.

- Respect copyright laws and intellectual property rights when using digital content.

- Report any IT issues or security incidents to the college's IT support.

- Comply with acceptable use policies and guidelines for internet, email, and software usage.

Password Security:

- Users should create strong passwords, consisting of a combination of uppercase and lowercase letters, numbers, and symbols.

- Passwords should not be shared with anyone and should be kept confidential.

- Users must change their passwords periodically, and password reuse across different accounts should be avoided.

- Multi-factor authentication should be enabled whenever possible to add an extra layer of security.

Reporting IT Issues:

- Users should promptly report any IT issues, malfunctions, or suspected security breaches to the designated IT support channels.

- Incidents involving unauthorized access, data breaches, or loss of sensitive information should be reported immediately to the appropriate authorities.

Adhering to Acceptable Use Policies:

- Users must familiarize themselves with and adhere to the college's acceptable use policies for IT resources, network access, email usage, and software licensing.

- Prohibited activities, such as accessing inappropriate content, engaging in cyberbullying, or violating copyright laws, must be strictly avoided.

Regular Training and Awareness:

- The college will provide regular training and awareness programs to educate users about IT policies, security best practices, and emerging threats.

- Users are encouraged to stay informed about evolving technology trends and potential risks associated with IT usage.

By understanding and fulfilling their responsibilities, users contribute to a secure and reliable IT environment at Marutraoji Ghule Patil College. These guidelines promote responsible IT practices, protect sensitive data, and create a culture of cybersecurity awareness among faculty, staff, and students.

III) Data Network Responsibilities of End Users:

End users, including faculty, staff, and students, have crucial responsibilities in maintaining the security and integrity of Marutraoji Ghule Patil College's data network. Adhering to these responsibilities helps protect against cybersecurity threats, unauthorized access, and ensures compliance with data protection regulations. The following guidelines outline the key responsibilities for end users:

1. Protecting Against Malware:

- Install and regularly update antivirus and anti-malware software on personal devices used to access the college network.
- Scan files and removable media for malware before transferring them to college systems.
- Exercise caution when downloading files or opening email attachments from unknown or suspicious sources.
- Report any suspected malware infections or unusual system behavior to the college's IT support.

2. Avoiding Unauthorized Access:

- Safeguard login credentials and avoid sharing passwords or account information with others.
- Use strong passwords and enable multi-factor authentication whenever possible.
- Do not leave devices unattended while connected to the college network.
- Log out or lock computers when not in use to prevent unauthorized access.
- Report any suspicious or unauthorized access attempts to the college's IT support.

3. Ensuring Compliance with Data Protection Regulations:

- Adhere to all applicable data protection regulations, including but not limited to GDPR, HIPAA, or FERPA, depending on the nature of the data being accessed or stored.
- Protect sensitive and confidential information by ensuring proper encryption, access controls, and storage methods.
- Use secure data transfer protocols (e.g., encrypted email or secure file transfer protocols) when transmitting sensitive data.

- Avoid storing sensitive information on personal devices or cloud storage solutions without proper authorization.

- Report any data breaches, incidents, or potential non-compliance with data protection regulations to the appropriate college authorities.

4. Regular System Updates and Patching:

- Keep operating systems, software applications, and firmware up to date by regularly applying security patches and updates.

- Enable automatic updates whenever possible to ensure the latest security features and bug fixes are implemented.

- Report any issues or difficulties in updating systems to the college's IT support.

5. Responsible Internet Usage:

- Access the internet through approved and secure networks, avoiding public or untrusted Wi-Fi networks.

- Exercise caution when visiting websites, downloading files, or clicking on links, as they may contain malicious content.

- Refrain from accessing or downloading unauthorized or copyrighted material.

- Report any suspicious or potentially malicious websites or links to the college's IT support.

6. Incident Reporting:

- Promptly report any cybersecurity incidents, such as phishing attempts, unauthorized access, or data breaches, to the college's IT support or designated incident response channels.

- Cooperate fully with any investigations or mitigation efforts following a security incident.

Regular Training and Awareness:

- The college will provide regular training and awareness programs to educate end users about data security best practices, phishing awareness, and emerging cyber threats.

- Users should stay informed about current security trends and remain vigilant against evolving cyber risks.

By adhering to these guidelines and fulfilling their responsibilities, end users play a vital role in maintaining a secure and reliable data network at Marutraoji Ghule Patil College. Their proactive measures contribute to the protection of sensitive information, prevention of unauthorized access, and compliance with data protection regulations.

IV) Computing Facility Provisioning and Maintenance:

Marutraoji Ghule Patil College recognizes the importance of providing reliable computing facilities, such as computer labs and servers, to support the academic and administrative activities of faculty, staff, and students. This section outlines the process for requesting and provisioning computing facilities and provides guidelines for their proper use, care, and maintenance.

1. Requesting Computing Facilities:

- Faculty and staff requiring access to specific computing facilities should submit a formal request to the appropriate administrative department or IT support.
- The request should include details such as the purpose of the facility, anticipated duration of usage, software requirements, and any additional resources needed.
- Requests will be reviewed, prioritized, and approved based on availability, resource allocation, and alignment with the college's goals and objectives.

2. Provisioning Computing Facilities:

- Upon approval, the IT department will provision the requested computing facilities, ensuring necessary hardware, software, and network connectivity are in place.
- Access privileges will be assigned based on the user's role and responsibilities.
- Users will be provided with login credentials and instructions for accessing and utilizing the facility.

3. Proper Use of Computing Facilities:

- Users should use the provided computing facilities solely for authorized academic or administrative purposes.
- Respect licensing agreements and use only legally acquired software on college-owned systems.
- Users should not attempt to modify or tamper with the hardware, software, or configurations of the computing facilities without proper authorization.
- Avoid installing unauthorized software or altering system settings that may compromise the stability, security, or integrity of the facilities.

4. Care and Maintenance of Computing Facilities:

- Users should handle computing equipment and peripherals with care, following manufacturer guidelines and best practices.
- Keep the computing facilities clean and free from food, drinks, and other substances that may cause damage.
- Report any hardware or software malfunctions, abnormalities, or damage to the IT support immediately.
- Regularly update and maintain installed software, including applying security patches and updates as directed by the IT department.
- Respect power-saving settings and shut down or log off properly after use.

5. Data Storage and Backup:

- Users should save their data on authorized network drives or storage areas provided by the college.
- Regularly back up important files to prevent data loss in case of hardware failure or system crashes.
- Avoid storing sensitive or confidential data on local drives or removable media unless authorized and necessary.
- Comply with college policies and guidelines regarding data retention, privacy, and security.

6. Security and Access Control:

- Users should protect their login credentials and not share them with others.
- Log out or lock computing facilities when unattended to prevent unauthorized access.
- Report any suspected unauthorized access, security breaches, or suspicious activities to the IT support.

7. Compliance with Copyright and Intellectual Property:

- Users must respect copyright laws and intellectual property rights when using computing facilities.
- Do not reproduce or distribute copyrighted materials without proper authorization.
- Adhere to college policies regarding the fair use of copyrighted materials for educational purposes.

By following these guidelines, users contribute to the proper use, care, and maintenance of computing facilities at Marutraoji Ghule Patil College. This ensures the longevity, reliability, and availability of these resources for the entire college community, fostering a productive and efficient academic and administrative environment.

V) Provision of Computing Software and Maintenance:

Marutraoji Ghule Patil College recognizes the importance of providing appropriate computing software to support the academic and administrative activities of faculty, staff, and students. This section outlines the procedures for software acquisition, licensing, and updates, and provides guidelines for software installation, usage, and restrictions to ensure compliance with copyright laws.

1. Software Acquisition and Licensing:

- The college's IT department is responsible for acquiring and managing software licenses for approved applications.
- Faculty and staff requiring specific software should submit a formal request to the IT department, providing details such as the purpose of the software, the number of licenses required, and any associated costs.
- The IT department will evaluate the request, ensuring compatibility, license availability, and adherence to licensing agreements and budget constraints.
- Once approved, the IT department will procure the necessary licenses and distribute them to the authorized users.

2. Software Updates and Maintenance:

- The IT department is responsible for monitoring software updates and patches to ensure security and functionality.
- Updates and patches will be applied in a timely manner to minimize vulnerabilities and optimize performance.
- Users should promptly install software updates as directed by the IT department to maintain a secure and stable computing environment.

3. Software Installation:

- Users should only install authorized software that has been approved and provided by the college.
- Unauthorized installation of software is strictly prohibited.
- Users should follow the designated installation procedures provided by the IT department or software vendor.
- Adhere to any special instructions or licensing agreements associated with the software.

4. Software Usage Guidelines:

- Users should use software for authorized academic or administrative purposes only.
- Respect copyright laws and intellectual property rights when using software.

- Do not reproduce or distribute software without proper authorization.

- Users must comply with the terms and conditions specified in the software license agreements.

- Sharing software licenses or using software on multiple devices without appropriate licensing is strictly prohibited.

5. Software Restrictions:

- Users should not attempt to modify, reverse engineer, or tamper with software code, licenses, or configurations without proper authorization.

- Use of software for malicious purposes, including hacking, unauthorized access, or any illegal activities, is strictly prohibited.

- Users should not install or use unauthorized software or tools that may compromise the security or stability of the computing environment.

6. Reporting Software Issues:

- Users should promptly report any software-related issues, bugs, or malfunctions to the IT support or designated channels.

- Reports should include relevant details such as error messages, system behavior, and steps to reproduce the issue.

- Users should refrain from attempting to fix or modify software issues on their own without proper guidance or authorization.

Compliance with these guidelines ensures that software acquisition, licensing, and usage at Marutraoji Ghule Patil College are aligned with copyright laws, licensing agreements, and ethical standards. By following these procedures, users contribute to a secure and legally compliant software environment, promoting the efficient use of software resources and safeguarding intellectual property rights.

VI) Provision of Network Connectivity and Maintenance:

Marutraoji Ghule Patil College recognizes the critical role of network connectivity in supporting academic and administrative activities. This section explains how network connectivity is provided and managed within the college and addresses issues related to network access, bandwidth usage, and wireless connectivity.

1. Network Infrastructure:

- The college's IT department is responsible for designing, implementing, and maintaining the network infrastructure.

- The network infrastructure includes routers, switches, cabling, access points, and other necessary equipment.

- The IT department ensures the network infrastructure is scalable, secure, and capable of meeting the college's current and future needs.

2. Network Access:

- Faculty, staff, and students are provided with network access credentials based on their roles and responsibilities.
- Access to the college's network is granted to authorized users, and access privileges are defined based on specific requirements.
- Users must protect their login credentials and not share them with others.
- The IT department reserves the right to restrict or revoke network access in case of policy violations or security concerns.

3. Bandwidth Usage:

- Users should use network bandwidth responsibly and refrain from engaging in activities that excessively consume bandwidth, impacting the overall network performance.
- Bandwidth-intensive activities, such as downloading large files or streaming high-definition videos, should be performed judiciously to avoid congestion.
- The IT department may enforce bandwidth management policies to ensure fair and optimal network performance for all users.

4. Wireless Connectivity:

- The college provides wireless connectivity in designated areas to facilitate flexible and convenient access to the network.
- Users should connect to the authorized wireless networks using their designated credentials.
- Users should follow wireless network usage guidelines and avoid activities that may compromise network security or disrupt the wireless environment.
- Wireless connectivity is subject to availability and may vary depending on the location and capacity of wireless access points.

5. Network Security:

- The college employs security measures to protect the network infrastructure and users' data.
- Firewalls, intrusion detection systems, and other security mechanisms are implemented to safeguard against unauthorized access, malware, and other threats.
- Users should adhere to network security policies, including not attempting to bypass or circumvent security measures.
- Report any suspected security incidents or network vulnerabilities to the IT department

immediately.

6. Network Maintenance:

- The IT department regularly maintains and monitors the network infrastructure to ensure its reliability and performance.
- Periodic assessments and upgrades are conducted to address emerging technologies, security vulnerabilities, and scalability requirements.
- Scheduled maintenance activities, including software updates, hardware replacements, and network optimizations, are performed to minimize disruptions.
- Users will be notified in advance of any planned network maintenance that may impact their access or usage.

7. Reporting Network Issues:

- Users should promptly report any network-related issues, disruptions, or performance problems to the IT support.
- Reports should include relevant details such as the time of occurrence, affected locations, and a description of the problem.
- Users should avoid attempting to resolve network issues independently without proper guidance or authorization.

VII) LAN and Internet Security:

Marutraoji Ghule Patil College recognizes the importance of securing the local area network (LAN) and intranet to protect sensitive data and ensure the confidentiality, integrity, and availability of resources. This section describes the security measures in place and provides guidelines for securing wireless networks, preventing unauthorized access, and handling sensitive data.

1. Securing Wireless Networks:

- Wireless networks should be secured using strong encryption protocols, such as WPA2 or WPA3, to prevent unauthorized access and eavesdropping.
- Wireless network access points should be properly configured with secure passwords and appropriate security settings.
- Default settings on wireless access points, such as default passwords or SSIDs, should be changed to unique and strong values.
- Regularly review and update wireless network security configurations to address any vulnerabilities or emerging threats.

2. Access Control and User Authentication:

- Access to the LAN and intranet resources should be restricted to authorized users only.
- Users should authenticate themselves using unique and strong passwords or other secure authentication methods, such as multi-factor authentication (MFA).
- User access privileges should be granted based on the principle of least privilege, ensuring that users only have access to resources necessary for their roles and responsibilities.
- User accounts should be regularly audited, and inactive accounts should be disabled or removed to minimize the risk of unauthorized access.

3. Network Segmentation and VLANs:

- Implement network segmentation and virtual LANs (VLANs) to segregate different user groups, departments, or sensitive data from one another.
- VLANs help prevent unauthorized access and limit the potential impact of a security breach by containing it within a specific network segment.
- Apply appropriate firewall rules and access controls between VLANs to regulate the traffic flow and enforce security policies.

4. Intrusion Detection and Prevention:

- Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic, identify suspicious activities, and block or mitigate potential attacks.
- Regularly update and maintain IDPS systems to ensure they are capable of detecting and preventing the latest known threats.
- Configure IDPS systems to generate alerts or notifications to promptly respond to potential security incidents.

5. Handling Sensitive Data:

- Users should handle sensitive data in accordance with applicable laws, regulations, and college policies.
- Use encryption methods, such as Transport Layer Security (TLS), to protect data transmitted over the LAN and intranet.
- Avoid storing sensitive data on local drives or devices without proper encryption or authorization.
- Implement access controls and permissions to restrict access to sensitive data to authorized personnel only.
- Regularly back up sensitive data and store backups securely to prevent data loss or unauthorized access.

6. Regular Security Audits and Assessments:

- Conduct regular security audits and assessments of the LAN and intranet to identify vulnerabilities, weaknesses, or gaps in security controls.
- Perform penetration testing to evaluate the effectiveness of security measures and identify potential entry points for unauthorized access.
- Address identified vulnerabilities and implement necessary remediation measures promptly.

7. User Awareness and Training:

- Provide regular cybersecurity awareness training to users to educate them about best practices, security policies, and the importance of safeguarding the LAN and intranet.
- Train users to recognize social engineering attacks, phishing attempts, and other common security threats.
- Encourage users to report any suspicious activities or potential security incidents to the IT department.

By implementing these security measures and following the provided guidelines, Marutraoji Ghule Patil College ensures the protection of the LAN and intranet, safeguarding sensitive data, and reducing the risk of unauthorized access or breaches. Regular monitoring, updates, and user education are essential to maintaining a secure network environment.

VIII) Provision of Network Services:

Marutraoji Ghule Patil College provides various network services to support the academic and administrative activities of its faculty, staff, and students. This section lists the network services offered and provides guidelines on their appropriate usage, as well as any restrictions or limitations.

1. Email Services:

- The college offers email services to facilitate communication and collaboration among users.
- Email accounts are provided to faculty, staff, and students for official college-related communication.
- Users should use college-provided email accounts for official correspondence and adhere to email usage policies and guidelines.
- Respect the privacy of others and refrain from sending unsolicited or inappropriate emails.

2. File Sharing and Storage:

- The college provides network-based file sharing and storage services to facilitate document collaboration and data sharing.
- Users should store and share files on authorized network drives or storage areas provided by

the college.

- Avoid storing sensitive or confidential data on local drives or removable media unless authorized and necessary.

- Follow file naming conventions, folder structures, and access control mechanisms defined by the college.

3. Printing Services:

- Printing services are available to faculty, staff, and students for academic and administrative purposes.

- Users should utilize printing services responsibly and avoid excessive printing to conserve resources.

- Follow the designated printing procedures, including selecting appropriate print options and collecting printed materials promptly.

4. Internet Access:

- The college provides internet access to authorized users for educational and research purposes.

- Users should use internet access responsibly, adhering to college policies and guidelines.

- Avoid accessing or sharing inappropriate, offensive, or illegal content that violates college policies or applicable laws.

- Respect copyright laws when accessing or sharing online materials.

5. Virtual Private Network (VPN):

- The college may provide a Virtual Private Network (VPN) service for secure remote access to internal resources.

- Users should only use the VPN service for authorized purposes and follow the established VPN usage policies.

- Protect VPN credentials and avoid sharing them with unauthorized individuals.

6. Voice and Video Communication:

- The college may provide voice and video communication services, such as VoIP or video conferencing.

- Users should utilize these services for authorized communication purposes, such as meetings, collaborations, or academic activities.

- Respect the privacy of others during voice or video calls and adhere to the college's communication policies.

7. Remote Access Services:

- The college may provide remote access services, allowing users to access resources from off-campus locations.

- Users should use remote access services responsibly and comply with the college's remote access policies.

- Protect remote access credentials and avoid sharing them with unauthorized individuals.

8. Other Network Services:

- The college may offer additional network services, such as intranet portals, online learning platforms, or specialized applications.

- Users should utilize these services according to their intended purposes and in compliance with associated usage policies.

- Follow any specific guidelines or restrictions related to the use of these services.

It is important for users to familiarize themselves with the guidelines and policies associated with each network service provided by Marutraoji Ghule Patil College. By using these services responsibly, users contribute to an efficient and secure network environment and ensure fair access and resource utilization for all members of the college community.

IX) Network Activities Not Permitted Over the Campus Network:

Marutraoji Ghule Patil College strictly prohibits certain network activities to maintain a secure and productive network environment. Users are expected to adhere to the following guidelines and refrain from engaging in activities that are considered violations. This section specifies the network activities not permitted over the campus network, along with the consequences of violating these prohibitions.

1. Unauthorized File Sharing:

- Engaging in unauthorized file sharing, including sharing copyrighted material, pirated software, or other intellectual property without proper authorization, is strictly prohibited.

- Users should respect copyright laws and only share files with appropriate permissions or licenses.

2. Hacking and Unauthorized Access:

- Attempting to gain unauthorized access to systems, networks, accounts, or data is strictly prohibited.

- Users should not attempt to bypass security measures, exploit vulnerabilities, or engage in any form of hacking activities.

- Unauthorized access or attempts may result in legal consequences and severe disciplinary actions.

3. Accessing Inappropriate or Offensive Content:

- Accessing or distributing content that is inappropriate, offensive, discriminatory, or violates college policies is strictly prohibited.
- Users should not visit or share websites, files, or any other content that contains explicit material, hate speech, or violates ethical standards.
- Respect the acceptable use policy and ensure that online activities align with the college's values and mission.

4. Unauthorized Network Monitoring or Interference:

- Users should not engage in unauthorized network monitoring, sniffing, or capturing of network traffic without proper authorization.
- Interfering with network operations, disrupting services, or attempting to compromise the integrity of the network is strictly prohibited.

5. Malicious Activities:

- Engaging in any malicious activities, such as spreading malware, viruses, or participating in distributed denial-of-service (DDoS) attacks, is strictly prohibited.
- Users should not introduce or distribute any malicious software or engage in activities that compromise the security or availability of network resources.

6. Spamming and Phishing:

- Sending unsolicited bulk emails, chain letters, or engaging in phishing attempts to deceive or obtain sensitive information from others is strictly prohibited.
- Users should not participate in any form of spamming or phishing activities.

Consequences of Violations:

- Violations of the network activities mentioned above may result in disciplinary actions, as outlined in the college's policies and codes of conduct.
- Consequences may include, but are not limited to, warnings, temporary or permanent loss of network access privileges, academic penalties, suspension, or legal actions as deemed appropriate.
- The severity of the violation, the intent, and the impact on the college's network and community will be considered when determining disciplinary actions.

Marutraoji Ghule Patil College is committed to maintaining a secure and productive network environment. Users must understand and respect the network activities that are not permitted. By complying with these guidelines, users contribute to the overall security, reliability, and ethical use of the campus network.

X) Violations:

Marutraoji Ghule Patil College takes violations of the IT policy seriously and has established procedures for reporting and addressing such violations. This section describes the procedures for reporting policy breaches and outlines the disciplinary actions that may be taken in response to these violations.

1. Reporting Violations:

- Any member of the college community who becomes aware of an IT policy violation should report it promptly to the appropriate authority.
- The designated authority for reporting IT policy violations may vary depending on the nature of the violation. This could include the IT department, faculty or staff supervisors, or the college's disciplinary committee.
- Reporting mechanisms may include submitting a formal complaint, contacting the IT helpdesk, or following the established reporting channels defined by the college.

2. Investigation and Review:

- Upon receiving a report of an IT policy violation, the college will initiate an investigation to gather relevant information and evidence.
- The investigation may involve reviewing system logs, interviewing witnesses, and examining any available digital or physical evidence.
- The investigation will be conducted by authorized personnel with the necessary expertise and authority.

3. Disciplinary Actions:

- The disciplinary actions taken in response to IT policy violations will depend on the severity of the breach, the impact on the college community, and any previous violations by the individual.
- Disciplinary actions may include, but are not limited to, the following:

a. Verbal or written warning: A warning may be issued for minor or first-time violations to educate the individual about the policy and emphasize the importance of compliance.

b. Loss of privileges: In cases where the violation is significant or repeated, the individual may have their access to IT resources, such as network access, email, or specific services, temporarily or permanently revoked.

c. Academic penalties: In situations where the violation relates to academic integrity or unauthorized assistance in coursework, the college's established academic penalty policies will be followed.

d. Suspension: For severe or repeated violations, the individual may be suspended from the college for a specified period, during which they will not be allowed to participate in any college activities.

e. Termination of employment or expulsion: In cases involving staff or faculty members, termination of employment may be considered. Similarly, for students, expulsion from the college may be the ultimate consequence for serious or persistent violations.

f. Legal action: In situations where the violation involves illegal activities, the college may involve appropriate law enforcement agencies, and legal consequences may apply.

4. Appeals Process:

- The college may provide an appeals process for individuals who believe they have been wrongly accused or feel the disciplinary actions taken against them are unjust.
- The appeals process, if available, will be outlined in the college's policies and provide a fair and impartial review of the case by an independent body or committee.
- The decision reached through the appeals process will be final and binding.

It is important for all members of the college community to understand and comply with the IT policy. By reporting violations and addressing them promptly and appropriately, Marutraoji Ghule Patil College ensures a secure and responsible IT environment that aligns with its mission, values, and legal obligations.

+ + +