Ref. No. Date 18/06/2024

IT POLICY

An **IT Policy** serves as a comprehensive framework that governs the use of information technology resources within institution. It ensures the effective, ethical, and secure utilization of IT infrastructure for educational, administrative, and research purposes.

1. Objectives

- Ensure the secure and efficient use of IT resources.
- Promote responsible use of digital tools and technologies.
- Safeguard sensitive institutional and personal data.
- Support academic freedom while complying with legal requirements.
- Facilitate smooth integration of IT services in teaching, learning, and administrative activities.

2. Scope

This policy applies to:

- All faculty, staff, students, and visitors using IT resources.
- IT infrastructure, including hardware, software, networks, and data systems.
- Both on-premises and cloud-based services.

3. Acceptable Use Policy

- IT resources are provided primarily for educational, research, and administrative purposes.
- Users must comply with institutional, national, and international IT laws.
- Unauthorized activities, such as hacking, spamming, or accessing prohibited websites, are strictly prohibited.

4. IT Infrastructure Management

4.1 Network Usage

- Only authorized devices are permitted to connect to the college network.
- Bandwidth usage should prioritize academic and administrative tasks over recreational activities.

- Use of personal hotspots is discouraged within campus premises to ensure network security.

4.2 Internet Access

- Internet access is monitored for security and compliance with usage policies.
- Access to harmful or inappropriate content is blocked.

4.3 Hardware and Software Management

- All hardware and software must be approved and installed by the IT department.
- Unauthorized software installations are prohibited.
- Licensing agreements for all software must be strictly adhered to.

5. Data Security and Privacy

- **Data Protection**: All institutional data must be securely stored and backed up regularly.
- **User Accounts**: Accounts should have strong passwords that are changed periodically.
- **Confidentiality**: Personal and academic data must not be shared without explicit permission.

6. IT Support and Maintenance

- An IT helpdesk will handle troubleshooting and system maintenance.
- Regular audits of IT infrastructure will be conducted to identify and address vulnerabilities.

7. Cybersecurity

- Firewalls, antivirus programs, and intrusion detection systems must be in place.
- Users must report any cybersecurity breaches immediately.
- Regular awareness sessions on cybersecurity practices will be organized.

8. Email and Communication Policy

- Official communication must be conducted using institutional email accounts.
- Bulk emails require approval from the administration.
- Avoid sharing sensitive information over unsecured communication channels.

9. Social Media and Digital Ethics

- Use of social media should align with the college's ethical guidelines.
- Institutional accounts should represent the college professionally.

10. BYOD (Bring Your Own Device) Policy

- Personal devices can be used for academic purposes but must adhere to network security protocols.
- IT department reserves the right to monitor network activity for compliance.

11. Policy Violation and Disciplinary Actions

- Violations of the IT policy may result in:
  - Revocation of IT privileges.
  - Disciplinary action as per the college's code of conduct.
  - Legal action in case of criminal offenses.

12. Review and Updates

- The IT policy will be reviewed annually to keep pace with technological advancements and legal changes.
- Feedback from stakeholders will be incorporated into updates.

SECRETARY