S. P. MANDALI's

RAMNARAIN RUIA AUTONOMOUS COLLEGE

POLICY FOR THE USAGE OF IT RESOURCES

Name of the organization: S P Mandali's Ramnarain Ruia Autonomous College
Policy Number: RRAC-Admin P-2

_____

Title of the Policy: Policy for the Usage of IT Resources

Effective Date : 2017-18

Last Revision Date:

Responsible Party: Principal, Management, IQAC, IT Department

Scope and Audience: Students, Administrative staff and Faculty

_____

1. Purpose

The Information Technology (IT) Usage Policy outlines guidelines for the responsible use of IT resources at Ramnarain Ruia Autonomous College. It ensures a secure, ethical, and legal use of IT infrastructure, promotes a productive learning environment, and safeguards institutional data.

2. Scope

This policy applies to all students, faculty, staff, and any external individuals or entities granted access to the college's IT systems, including hardware, software, internet access, email services, and network resources.

3. Acceptable Use

- **Educational and Administrative Purposes:** IT resources must primarily be used for academic, administrative, and research activities in line with the objectives of the college.

- **Ethical Conduct:** Users must behave ethically and responsibly when accessing or using IT resources, ensuring respect for intellectual property, privacy, and legal requirements.

- **Institutional Use:** All IT equipment and services provided by the college should be used strictly for institutional purposes, not for personal or commercial activities.

4. User Responsibilities

- **Access Credentials:** Users are responsible for maintaining the confidentiality of their login credentials. Sharing login information is prohibited.

- **Data Protection:** Users must ensure that sensitive information, including personal data and research material, is protected from unauthorized access or disclosure.

- **Copyright Compliance:** All digital content used must comply with copyright laws. Downloading or sharing copyrighted material without permission is prohibited.

- **Software Licensing:** Only authorized and licensed software is allowed. Users should not install, download, or distribute software without prior approval from the IT department.

5. Compliance with Legal and Regulatory Standards

- **Legal Compliance:** The College will comply with all applicable IT laws, including data protection regulations (e.g., the Information Technology Act, 2000), intellectual property laws, and guidelines related to online conduct. Any identified non-compliance will be reported to the College administration, and corrective measures will be taken promptly.

- **Data Privacy:** The institution will adhere to laws concerning the collection, storage, and use of personal data, ensuring compliance with data privacy and protection standards.

6. IT Support and Maintenance

- **Help Desk Support:** A dedicated IT support team will be available to assist users with any technical issues, software installation, or network connectivity problems. The help desk can be contacted via email, phone, or in person.

- **Maintenance Schedule:** Regular maintenance of IT systems will be conducted to ensure optimal performance. Users will be notified in advance of any planned downtime for system upgrades or repairs.

- **Incident Reporting:** Users should report any IT-related incidents, such as system malfunctions, data breaches, or unauthorized access, to the IT department immediately for prompt resolution.

7. Prohibited Activities

- Unauthorized Access: Users must not attempt to access restricted areas of the College's IT systems or network.

- Malicious Activity: Any activity that harms or disrupts the IT environment, such as spreading viruses, hacking, or unauthorized monitoring, is strictly forbidden.

- Inappropriate Content: Accessing, sharing, or distributing offensive, obscene, or inappropriate content is not allowed.

- Network Misuse: Excessive use of bandwidth for non-academic purposes (e.g., streaming, gaming) that hinders network performance for others is prohibited.

8. Email and Communication Services

- Professional Use: College-provided email accounts should be used for official communication only. All communications should follow professional and respectful standards.

- Spam and Phishing: Users must be cautious of suspicious emails and report potential phishing attempts to the IT department.

9. Privacy and Monitoring

- Monitoring: The College reserves the right to monitor IT usage to ensure compliance with this policy. However, it will respect users' privacy as far as possible and only access personal data for legitimate reasons.

- Personal Devices: Users connecting personal devices to the College network must ensure they are secure and free from malware. The College may require users to disconnect devices that pose a security risk.

10. Data Security and Backup

- Data Storage: Critical institutional data will be stored on approved College servers or cloud storage, not on personal devices or third-party platforms.

- Backup: The College will ensure regular backups of institutional data. Users are responsible for backing up personal data stored on College systems.

11. Violations and Enforcement

- Reporting Violations: Suspected violations of this policy should be reported to the IT department or the appropriate College authorities.

- Consequences of Misuse: Misuse of IT resources may result in disciplinary actions, depending on the severity of the breach.

12. Policy Review and Updates

This policy will be reviewed periodically by the college administration and IT department to adapt to technological changes and emerging security challenges.

Prof. (Dr.) Anushree Lokur
Principal

Principal
Ramnarain Ruia Autonomous College
Matunga, Mumbai- 400 019