Ramakrishna Mission Sikshanamandira

A NCTE Recognized Govt. Aided (WB) Residential Autonomous Post Graduate College of Teacher Education Affiliated to University of Calcutta

College of Teacher Education (CTE)
College with Potential for Excellence(CPE)

Website: www.rkmsm.org; Email: rkmsmc@gmail.com
Phone: 033-2654 9281, 033-2654 6081

ICT POLICY

BELUR MATH, HOWRAH, WEST BENGAL, PIN: 711202

1.   Purpose and Scope:

Sikshanamandira is committed to providing modern Information and Communication Technology (ICT) resources to make all its activities smooth, secured, robust and well connected. For that reason Sikshanamandira's ICT policy is devised to fulfil the below **purposes -**

1) Outline of acceptable use (and misuse) of Institutional ICT resources.
2) Enhancing daily administrative & academic activities through effective implementation of digital connectivity as well as maintaining segregation and user/ departmental privacy with regards to all confidential transactions & communications between department, administration and clients.
3) Protecting and safeguarding the digitally born and other soft resources of the Institution, the scope of which incorporates the measures to ensure inter-personal & inter-departmental data protection as well.

The **scope** of policy applies to users of RKMSM ICT resources & networks including, but not limited to:
1. Students;
2. Staff;
3. Contractors and consultants;
4. Visitors;
5. Affiliates and third parties.

Users that are connected to RKMSM networks or services must comply with this policy, irrespective of location or device ownership (e.g. personal computers, mobile devices, etc.).

2.   Available ICT Resources & Related User Policies:
2.1.   College Servers & Wifi:
    2.1.1.   The college has **Four dedicated servers -**
1. Administrative Server (covers CoEx, Hostel and Accounts)
2. Academic Server (covers Faculty desktops, classroom nodes, Library, Laboratory, Comp. Kiosk etc.)
3. Journal/ New Library Server (covers extended facilities provided by the Library including at Research Section)
4. Moodle Server covers the backend of the Institutional Moodle module accessible through the college website.

All computers of the College are connected to these servers accordingly through LAN connections.

    2.1.2.   The LAN connections throughout the campus are segregated to ensure interdepartmental and administrative confidentiality.

2.1.3. All the data in all computers are backed up in the **NAS** (WD cloud storage 16 TB). Therefore, the pertinent users must not keep any personal and inappropriate documents in such places either as it may compromise their privacy or should be considered as a breach of the CoC of the Institution respectively and may lead to appropriate action against the offender. Furthermore, they shouldn't load unnecessary large sized files so that the connection speed across the network are not compromised.

2.1.4. The whole campus is connected through Wifi. For the purpose of security, WiFi channels are also segregated for College Administration and the rest of the stakeholders.

2.1.5. Certain social media and other potentially hazardous, insecured, malicious and inappropriate sites are blocked off in the Wifi channels to ensure integrity and security. By using any means to circumvent these restrictions will lead to disciplinary action.

2.1.6. All The users in the college will have accessibility to Wifi connection and the bandwidth of the internet connection should suffice the requirements of the students, and staff.

2.2. Google Workspace (G Suite)

2.2.1. Each faculty, non teaching staff as well as Scholars are provided personal email accounts under the organizational workspace by the College through its **Google Workspace for Education (erstwhile G Suite)**. Some departments such as Controller of Examinations, IQAC, Accounts, Library, Publication, Hostel, Journal etc. have separate organizational emails dedicated for its departmental as well as transactional activities. The user policy regarding the organizational emails and workspace is as per the following -

    2.2.1.1. The workspace has an unlimited Google Drive, hence uploading official files and sharing/editing/storing is to be done through digital mode whenever applicable and suitable.

    2.2.1.2. The organizational account along with all its features are maintained by the college, hence it must be used **ONLY FOR OFFICIAL PURPOSES**.

    2.2.1.3. Using the Organizational account for social media, personal usage is prohibited and is subject to approval from college management.

    2.2.1.4. The college retains the discretion to suspend/discontinue any of the organizational addresses if it deems fit.

    2.2.1.5. On account of retirement/resignation/termination, the college resumes the right to suspend/discontinue pertinent account(s).

    2.2.1.6. All official correspondence to and fro with College administration should be via organizational emails only.

2.2.1.7. Additionally, an user/ department should sync the relevant account(s) to their smartphones/tablets/laptops for direct and prompt notification.

2.2.1.8. Google Classrooms for all academic activities should be created by the respective Faculty members under their organizational workspace account only.

2.2.2. As detailed above, each department has its own Google Workspace Setup as well as intra-departmental and interdepartmental network connectivity for all kinds of transactions. The users therefore are expected to make their internal transactions of documents and other information digitally in most cases.

2.3. Software Policy

2.3.1. In today's ICT world, there are numerous valid reasons to use Open Source software. In addition to costs and independence from software vendors (vendor lock-in), the high-quality software, competitive features and technical capabilities as well as adaptability are important features of Open Source software. Therefore, Sikshanamandira always encourages the use of open source software over licensed softwares.

2.3.2. Installation of pirated/ unlicensed software in the administrative computers are prohibited.

2.3.3. In addition, potentially malicious software which may cause threat to the institutional security are not to be installed and used in institutional computers.

2.4. CCTV Surveillance Policy

2.4.1. Purpose and Scope:

The purpose of this policy is to establish guidelines for the installation, use, and management of Closed Circuit Television (CCTV) cameras within Ramakrishna Mission Sikshanamandira, Belur Math, Howrah and hereafter referred to as "Sikshanamandira."

This policy applies to all CCTV cameras installed on the Institution's premises, including classrooms, libraries, common areas, and outdoor spaces.

2.4.2. Legal Compliance:

Sikshanamandira will adhere to all applicable laws and regulations, including the Information Technology Act, 2000, and the Right to Privacy under Article 21 of the Constitution of India, when implementing and operating the CCTV system.

2.4.3. Camera Placement:

CCTV cameras are strategically placed to enhance security, prevent vandalism, and protect the safety of individuals.
Cameras will not be installed in private areas, such as restrooms or changing rooms.
Camera locations will be determined in consultation with security experts and relevant authorities.

2.4.4. Notice and Consent:

The Institution will prominently display signs indicating the presence of CCTV cameras at all entrances and key areas.
Consent will not be required for general monitoring purposes, but it will be sought when specific individuals or groups are being monitored for legitimate reasons.

2.4.5. Data Protection and Privacy:

The Institution will respect the privacy rights of individuals. Cameras will not capture or store personal data unnecessarily.
Recorded footage will be used solely for security and safety purposes.

2.4.6. Data Retention:

CCTV footage will be retained for a maximum of 3 to 4 weeks unless required for investigative or legal purposes.
Retention periods will be consistent with applicable laws and regulations.

2.4.7. Access Control & Data Security:

Access to CCTV footage will be restricted to authorized personnel only. CCTV footage will be stored securely and encrypted to prevent unauthorized access or tampering.

2.4.8. Incident Reporting:

Any breaches or incidents related to the CCTV system, including unauthorized access or data leaks, will be reported to the designated authorities and investigated promptly.

2.4.9. Public Access:

CCTV footage will not be made publicly accessible unless required by law enforcement or other authorized entities.

2.4.10. Review and Updates:

This policy will be reviewed periodically and updated as needed to ensure alignment with evolving laws and regulations.

2.4.11. Third-Party Contractors:

If third-party contractors are involved in CCTV system maintenance or monitoring, they must adhere to the same privacy and security standards as outlined in this policy.

2.4.12. Enforcement:
Non-compliance with this policy may result in disciplinary action.

3. ICT Services & Responsibilities:

The ICT staff is responsible for:

3.1. Provisioning ICT resources (e.g. user accounts, file storage, access to systems, printers, scanners);

3.2. Attending to IT requests and queries on a day-to-day basis;

3.3. Monitoring the use of resources to determine violations of authorised use;

3.4. Technical enforcement of this policy including –

3.4.1. Preventing and monitoring access to inappropriate content;

3.4.2. Suspending user access when required and approved by Administration;

3.5. Complying with local standard operating procedures where applicable.

4. ICT Service Management System:

The college has the following ICT Management System as mentioned below -

4.1. A two-member team (college staff) under the Maintenance Department looks after the maintenance of the IT service at the primary level on a day-to-day basis. There are separate slips available at the Maintenance Dept. office for repair/ maintenance/ replacement/ new purchase regarding ICT resources as well as Software related issues. Any stakeholder including Teaching & Non Teaching Staff as well as Ph.D. Scholars and Students are to duly fill in the specific slip and submit it to the Maintenance Department as well to communicate their issues to the designated Staff. Upon the consent from the Head of the Maintenance Department, their issues shall be resolved with due priority.

4.2. More comprehensive IT service is provided by different registered external companies each on an Annual Maintenance Contract. The college has Threefold AMC coverage -

4.2.1. For overall College Network, College computers, Biometric systems (including data capture & maintenance) and CCTV systems (including record maintenance).

4.2.2. For ICT infrastructure such as photocopier machines and PBX.

4.2.3. For website maintenance & associated services such as Admission portal.

4.3. Problems affecting IT products under warranty are referred to the concerned manufacturing companies for redress.

5. Security Measures Undertaken:

Security issues related to ICT are handled with the following measures:

5.1. All confidential data are password protected.

5.2. Data related to the accounts section, the examination section and the library are backed up separately.

5.3. The general network service is password protected.

5.4. Making all users aware of keeping their passwords and other confidential data private.

5.5. The LAN systems are firewall protected. Additional firewalls on the PC can also be enabled for enhanced security.

5.6. Installation of Antivirus Softwares (Microsoft Security Essential, Quick Heal, Kaspersky, McAfee).

5.7. As mentioned in the 'ICT Resource & Related Policy' section, the overall LAN connections as well as the WiFi channels have proper segregation in place so that there is a division between Students & Other Clients, different Departments & Faculty Members and the College Administration. This measure is taken to uphold security and confidentiality of all parties.

6. Misuse of ICT Resources:

The College Administration has the provision to authorise an investigation into alleged misuse. If allegations are deemed to be valid and of a serious nature, evidence of misuse will be reported to the appropriate body. A formal disciplinary action may be taken against the person violating the rules.

7. E-Governance:

For quick and effective information exchange and dissemination, the college has implemented an e-Governance platform wherever it is applicable and feasible. Such implementations include but not limited to:

7.1. For safety and security reasons, the Controller of Examination section has a separate Examination ERP exclusively for the maintenance of academic records of the students.

7.2. The Accounts Department works with a dedicated accounting software (such as **Tally ERP**) accessible only to the Accounts Department..

7.3. Administration uses the exclusive Admission ERP for all admission related purposes & issues.

7.4. There is also provision for Faculty members to use Moodle - a free and open-source learning management system that the college has implemented to some extent as a repository for Digital Study Material.

7.5. Notifications and other administrative communications are done only through Organizational e-mails and other digital modes available within the Organization Google Workspace Features.

8. Upgradation of ICT Infrastructure:

The plans and strategies for deploying and upgrading the IT infrastructure are guided by the requirements placed by the students, researchers, teachers and office staff.

Swami Vidyamritananda
Principal (Offg.)

Swami Vidyamritananda
Principal (Offg.)
Ramakrishna Mission Sikshanamandira
Belur Math, Howrah-711202, W.B.