POLICY ON INFORMATION TECHNOLOGY

Document Number: RPRA/POL/06

Date of release by IQAC:

Reviewed by	Approved by	Date of release
IQAC	GC Members	
Date: 7/9/16	Date: 10/9/16	Date: 11/9/16.

Prepared by

1. Dr. K. Suresh Babu, CSE, Professor & HOD,
2. V. Rajesekhar, CSE, Asst. professor – VRaj
3. G. Satish Kumar, CSE, Asst. Prof —

POLICY ON INFORMATION TECHNOLOGY

Introduction

In order to construct, manage, secure, and assure the legal and acceptable usage of the information technology infrastructure built on the college campus, IT policy is required. In accordance with this policy, the college creates methods and responsibilities for safeguarding the Privacy, Authenticity, and Accessibility of the data assets that are accessed, generated, maintained, and/or managed by the college. Data, data management, computers, network equipment, copyrighted material, as well as papers and verbally delivered information, are all examples of information assets covered by the policy.

Objectives

- Use of these facilities is monitored to provide a safe computing environment, as well as to adhere to regulatory regulations.
- A "user" is defined as any individual, group, or organization that falls under the control of the RISE Krishna Sai Prakasam Group Of Institutions, including students, employees, professors, departments, and offices.
- Users are obligated to adhere to any and all rules and regulations that may be issued from time to time by the Institution.
- Designed for internal use, this document is accessible to all users.

Responsibilities of users and user groups

- Federal, state, and any relevant laws must be adhered to by all users.
- Enforcing intellectual property and commercial software copyright rules.
- Ensuring compliance with all applicable rules and regulations regarding government, telecommunications, and networking.
- Honoring the acceptable usage rules of networked computers accessed through the RISE campus network, both locally and remotely.
- It is possible to ensure that all students have equitable access to the campus network resources by eliminating unnecessary network traffic

The supply and upkeep of computing facilities.

- User computer facilities are provided and maintained by the ITC (IT COMMITTEE). The user is granted access to the facilities once the management has given their consent.
- Ensure that the equipment is physically safe and manufacture it as needed by ITC for stock verification. The user must notify ITC if any of the allocated equipment's peripherals or

components is missing so that ITC can take appropriate action.

- ITC should be notified before any extra devices are plugged onto LAN. This may also be used to connect external devices, such as USB, to external ports.
- If a user's personal peripherals fail to connect to institute equipment, ITC will not be held accountable.
- Taking frequent backups of data saved on a user's PC is the best way to assure data availability and security.
- It is the individual's or the department's responsibility to notify ITC of any software / hardware issues using the reporting mechanisms provided. ITC will do all in its power to have this issue resolved as soon as possible. In some cases, competent authorities may be required to authorize repairs that involve a significant financial investment.
- There should be a record of every support call that is handled by an employee.
- The College retains ownership of any equipment that is assigned to a person or a department.
- Student use of computers on campus will be controlled by the regulations of the College, not the policies of the University. As a result, students must adhere to the IT policy when using campus-owned computers and other technology.

The provision and upkeep of computerized tools

- Device management software is provided by ITC for each user's use.
- In order to protect the Institute's equipment, ITC has the authority to safeguard all of the administrator passwords.
- Prior authorization from ITC is required before users may put any application on the device they are given. However, ITC has the right to prevent user from accessing any programme that might expose the confidentiality and reliability of the campus network.
- All applications installed on user computers must be legitimate versions from the original manufacturers. Any unauthorized or unlicensed programme should not be used by anybody, including users.
- It is ITC's responsibility to reinstall applications in the event that it is necessary. Requests for help can be made using the facilities available to make them.
- College-owned or downloaded software may not be copied, reproduced or distributed **by users.**

The maintenance and provision of network connections

- From their facility to all college network services, ITC is accountable for supplying data communication access.
- It is the responsibility of ITC to plan, build, create, and maintain campus-wide network infrastructure that connects all users.
- Proactive monitoring by ITC of shared networks will uncover issues and ITC will take the required procedures to isolate and remedy the problem.
- It is the responsibility of the user to register their own devices with the ITC before they may be linked to the network.

Network policies

Users are not allowed to share their passwords, software licencing codes, or other security codes with anybody else. Passwords should be changed every 90 days in order to keep users' accounts safe and secure. Changing all system-level (root, enable, network administrator) passwords at least once every 90 days is required.

Using RISE internet services to view, access, save or communicate pornographic material of any type is expressly forbidden.

- Violence or threats of violence.
- Activities that are not permitted by law.
- Messages from the ad world
- Statements of a sociopolitical or ethnic nature.
- Gambling.
- Gaining money for oneself.
- Sending out email chains.
- Spamming e-mail accounts using RISE e-mail services or machines.
- When opening files acquired from the Web without first completing a malware scan..
- Without permission from the ITC, downloading and/or executable files on any network computers.
- ITC may shut down the internet services from time to time for maintenance purposes.. In the event of a system outage, users will be notified in advance.

Violations

- Violations will be looked at on an individual case-by-by-case basis.
- One or more violations of the foregoing use limits will result in a warning from his or her department head or reporting authority, and the user's ongoing use will be closely watched.
- The Manager will take quick action if a serious violation has occurred. Loss of Internet and/or email rights, harsh censure, and/or disciplinary action is all possible outcomes of such behavior.
- During an investigation into an alleged rule violation, a user's computing and communication access may be restricted.
- In the event of a conflict or disagreement, the management's decision is final and binding.