IT Policy: Table of Contents

Policy Purpose :

The purpose of this document is to inform the stakeholders (Faculty, Students, Support Staff, Alumnus, Guests etc) of Rishi Dayaram & Seth Hassaram National College and Seth Wassiamull Assomul Science College affiliated to University of Mumbai and under the H.S.N.C.B. (R.D. & S.H. National College) of what can be expected in terms of Information Technology (IT). With increasing use of technology, there is a need for legal, secured, process to procure, use and maintain the IT infrastructure. IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, faculty, support Staff, Management and visiting Guests.

This covers the use of the following infrastructure resources

- Computer Hardware: Servers, Computers, printers, wireless devices etc.
- Network Devices: Firewalls, Routers, Managed Switches, Access Points
- Computer Software
- Security and Surveillance Cameras
- ICT infrastructure tools

Policy Statement

Authorized users of R.D. & S.H. National College use computers, communication devices, E-Mail, Internet resources (collectively the "Information Resources ") for assisting them in performing the teaching and administrative work, education purposes. Use of these Information Resources for any purpose that is not specifically related to these purposes is prohibited.

Hardware and Software Purchase Policy

IT infrastructure resources are categorized as hardware and software resources. Purchase of any new product is monitored by the Purchase committee in consultation with the Principal and the Finance Officer.

The Purchase committee comprises

- Secretary of the HSNCB
- Head of the Institution
- Convener of the Purchase Committee
- Staff Members with IT knowledge
- Network Engineer
- Convener Website Committee
- Finance Officer in Charge of the Institution

The need-based requirement is obtained from the Departments and administration. The technical specifications needed are prepared by the purchase committee. The specifications are sent to at least three service providers and vendors and the quotations are obtained on institutional e-mail ID or directly in a sealed envelope. The purchase committee compares the quotations received and prepares a purchase order which is signed by the Principal and the Convener of the purchase committee. Separate meetings with the vendors are scheduled for any clarifications. The purchase order is sent to the selected vendor. All Computers purchased are with 3 year onsite comprehensive warranty.

The open-source Software required as per the syllabus is downloaded from the official websites and installed on the required Computer systems by the Laboratories in Charge after discussions with faculty members.

For uploading information on the website and allocation of E-Mail from the College domain, the requests are made to the website administrator. The administrator would upload the material on the website after verifying the material.

IT Infrastructure Resources

Software Resources

- Licensed Operating System
- Software Licenses of Application Software
- Antivirus License
- License for Firewall
- License for Wi Fi Management
- College Domain (for the Website)
- Open-source Software tools
- License for online educational tools

Hardware Resources

- Desktop Computers
- Laptop Computers
- Switches
- Firewall
- Access Points
- Equipment for Leased line connectivity
- Surveillance Security Cameras
- ICT Teaching – Learning Tools
- Web Conferencing Tools

- Other miscellaneous devices: Printers, Scanners, Copiers, Duplo Machines, Projectors, Smart Boards etc.

Hardware and Software Procurement Policy

Once the product is delivered, it is received by the IT person. The product is tested and accepted. The stock entry is made. The required installations and testing procedure are completed.

Device Allocation Policy

The product is then sent to the concerned department. The allotment record entry is added for allocation. The Head of the Department /Course Coordinator /In-Charge of the facility will receive the product. Hardware equipment is installed in designated places. Training if required is arranged for intended users of the product. Software packages are downloaded and installed by the network administer only.

Software Licensing and Installation Policy:

- Wherever possible the institution encourages the user community to go for open-source software where updates to the latest technology is readily available.
- The license key for software purchased is obtained on the Institutional E -Mail ID.
- The license key and details of installation are given to the departments and installations are carried out by authorized employees only after preparing a schedule.
- Individual users should make sure that respective computer systems have their Operating Systems updated regarding their service packs/patches, through the Internet for any bug fixes and vulnerabilities in the Operating Systems.
- Once the installation is complete, it is tested by members of staff who are going to use the product.
- Software licenses are renewed after a fixed time, depending upon the purchase agreement.
- The Institution / Department maintain a record of software licenses purchased. The following details are maintained.
    - Details of License key along with purchase details

  - Date of activation of the license.
  - Validity of the License
  - Serial Number of devices on which the software is installed.

- **Operating System and its updating:** Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through Internet.

- Computer systems used in the institutions should have antivirus software installed which should be active all time.

- Regular backups of their important data should be done by individual users.

Network Use Policy:

- The maintenance and support of the network is done by the institutional technical team.
- The problems related to the institutional network should be reported to the technical team.
- The technical assistant should assign an IP address to every computer system which is connected to the institutional network. Proper approach is used to allocate IP addresses. An IP address allocated to a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port.
- A proper server room is present in the institution's building. Server room supplies network connection in the institution building. There is a main network cable called Category 6 which shares internet connection.
- Network switches are present at proper places in buildings.
- Leased Line is installed on the campus.
- Access Points for Wi-Fi are installed in the campus , corridors and laboratories.

Website Policy:

This policy provides guidelines for the maintenance of all relevant technology issues related to the institutional website.

- Keeping the file up to date will be the responsibility of the Website Committee and the Chairman and will be responsible for any renewal of items listed in the file.

- All content on the institution website is to be accurate, appropriate, and current. This will be the responsibility of the Website Committee Chairman and the members of the Website Committee.

Website File Maintenance

- The website file must record the following details:
- List of domain names registered to the institution
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

Security Policy

- Internet Firewall is installed in the Wi Fi Server Room. Firewall facilitates various security policies.
- DHCP Configuration
- Blocking of Sensitive content
- User Creation and User Permissions
- Bandwidth Control Policy
- Antivirus
- Sensitive content and certain keywords are blocked for students
- Social Media Websites and search engines are disabled at the time of examinations.
- Separate SSID for Staff, Support Staff, Students and guests
- Need based Bandwidth Control
- Antivirus at the server side

Web Application Filter

Application	**Staff**	**Students**	**Support Staff**	**Guests**
Sites Blocked	Porn, torrents, Proxy & Hacking, Gambling, Marijuana, Criminal Activity			
YouTube	Allow	Need Based/Time Based	Allow	Allow
What's App	Allow	Need Based/Time Based	Allow	Allow
Facebook	Allow	Need Based/Time Based	Allow	Allow
Skype or Video calling	Allow	Need Based/Time Based	Allow	Allow
Entertainment	Allow	Need Based/Time Based	Allow	Allow
TV news Channel	Allow	Need Based/Time Based	Allow	Allow
Online Games	Deny	Deny	Deny	Deny
Windows Update	Allow	Allow	Allow	Allow

Default Block Category in Firewall

- Weapon
- Phishing and fraud
- Militancy and Extremist
- Gambling
- Pro-Suicide and self-Harm
- Criminal Activity
- Marijuana
- Intellectual Piracy
- Hunting and Fishing
- Legal highs
- Controlled substances

- Anonymizers
- Sexually Explicit
- Nudity
- Advertisement

User Policy for stakeholders

- Different types of users are identified for the IT systems installed in the college. Different users have different roles and responsibilities in the system.
- **Student Users:** Students are the end user of the system. They use the systems from the computer laboratories of the college. They have minimum permissions on the system. They can save their work, connect to the internet and use the installed software packages. Students do not have access to shared network resources like photo copy machines.
- **Teaching Staff Members:** They are the end users of the system. Like students, they also use the computer laboratory. They also use laptops, computers in classrooms and ICT tools. Teachers can also access other shared network resources like printers etc. They can also get access to security cameras with help of the network administrator.
- **Non-teaching staff members**: They are end users of the system. They mainly use the system for college administrative work like admission process, result processing etc. They have separate user id created for them.
- **Administrative staff members**: They are primary users of the system. Hierarchical structure is maintained in administrative staff members. Network administrator has full access to all systems including firewall and network. Web site and domain administrator has access to the domain to upload information on the website. Allocating email id to staff and students is also the responsibility of the web site and domain administrator. Four lab assistants are assigned as secondary users. They are assigned the tasks of software installations, updates and maintenance of the system.

Bring your own Device Policy:

- Employees are expected to protect personal devices used for work-related purposes from loss, damage, or theft.
- Institution will not be responsible for loss or damage of personal devices and applications.

Email Account Use Policy

- To increase the efficient distribution of critical information to all faculties, support staff and students, and the Institute's administrators, it is recommended to utilize the institute's e-mail services, for formal Institute communication and for academic and other official purposes.

- Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty, support staff, and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

- To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on with their Institutional User ID and password.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

- Using the facility for illegal/commercial purposes is a direct violation of the institute's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages and generation of threatening, harassing, abusive, obscene, or fraudulent messages/images.

- User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have potential to damage the valuable information on your computer.

- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

- Impersonating email account of others will be taken as a serious offence under the institute IT security policy.

- It is ultimately everyone's responsibility to keep their e-mail account free from violations of institute's email usage policy.

- The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., if they are being used from the institute's campus network, or by using the resources provided by the institute to the individual for official use even from outside.

Software and Hardware Maintenance Policy

- Software and Hardware Maintenance Policy Maintenance of IT infrastructure is taken up systematically and methodically.

- A regular stock update is taken at the end of each academic year. Any wear and tear of peripheral devices is recorded.

- All switches and electrical connections are checked once each month to avoid any electrical issues like short circuit.

- Software Maintenance Software patches are released daily. Some of them are installed automatically with active internet connection. If the automatic update option is not checked, then the software packages are required to be updated manually.

- A regular data backup is done by the lab assistant on a weekly basis.

- Open-source software also needs to run updates on a regular basis.

- If the license is renewable, and if the renewal is due, the network administrator will raise the request with the purchase Committee. Once the request is approved, software can be updated / new license can be obtained.

- Lab attendants perform a regular data clean up in the computer labs, library and the Network administrator performs a data clean-up operation on the college server. All temporary data is removed, all required data is restored in respective folders.

Disposal of Technology Equipment Policy

- The Institute is aware about the green initiative and proactively takes initiative in effective management of electronic waste generated.
- Electronic data files that contain confidential or private data should be deleted and completely removed from the trash, if applicable, as soon as they are no longer necessary.
- Electronic devices that may have confidential or private data and are ready for disposal must be drilled or destroyed.
- Network administrator must be notified of any IT equipment which is no longer required by the departments, as they can ensure whether the equipment can be reused or disposed of as appropriate.
- If the systems are unusable then they are dismantled and passed on for safe recycling of the e-waste to our E waste recycling partner.