Rathnavel Subramaniam College of Arts and Science

Autonomous and Affiliated to Bharathiar University, Approved by AICTE

Re Accredited with 'A' Grade by NAAC

SULUR, COIMBATORE

IT Policies & Guidelines

Table of Contents

IT Policy 2021

1. Need for IT Policy

The computing resources at Rathnavel Subramaniam (RVS) College of Arts and Science, Sulur, Coimbatore is intended to support the educational, instructional, research, and administrative activities of the college and the use of these resources is a privilege that is extended to the members of the RVS community. RVSCAS has network connections to every computer system covering all the academic and administrative buildings across the campus and hostel. RVS Infotech is the department that has been given the responsibility of running the College's intranet and Internet services and managing the network of the institution.

The IT policy of the college is formulated to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established on the campus and provide guidelines on acceptable and unacceptable use of IT resources of the college.

The IT Policy applies to technology administered by the college centrally, or by the individual departments, to information services provided by the college administration, or by the individual departments, or by individuals of the college community, or by authorized resident or non-resident visitors on their own hardware connected to the college.

This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centres, Laboratories, Offices of the college, recognized sub-units of the college and wherever the network facility is provided by the college. Computers owned by the individuals, or those owned by research projects of the faculty and students, when connected to campus network, are subjected to the 'Do's and 'Don'ts detailed in the IT policy. Further, all the faculty, students, departments, authorized visitors/visiting faculty and others who may be granted permission to use the information technology infrastructure of the college, must comply with the guidelines. Certain violations of IT policy by any member of the college community may even result in disciplinary action against the offender/s by the college authorities. If the matter requires the involvement of legal action, law enforcement agencies may also be informed.

Applies to

Stake holders on campus or off campus

- ❖ Students: UG, PG, and Research
- ❖ Faculty Members
- ❖ Administrative Staff (Non-Technical / Technical)
- ❖ Higher Authorities and Officers
- ❖ Guests

Resources

- ❖ Network Devices wired/ wireless
- ❖ Internet Access
- ❖ Official Websites, Web applications
- ❖ Official Email services
- ❖ Data Storage
- ❖ Mobile/ Desktop / server computing facility
- ❖ Documentation facility (Printers/Scanners)
- ❖ Multimedia Contents
- ❖ Surveillance network

2. IT Hardware Installation Policy

The network users need to observe certain precautions while getting their computers or peripherals installed so that they may face minimum inconvenience due to interruption of services due to hardware failures.

a) Primary User

An individual in whose room the computer is installed and is primarily used by him/her is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

b) End User Computer Systems

Apart from the client PCs, the College will consider servers not directly administered by RVS Infotech, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users.

Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the RVS Infotech, are still considered under this policy as "end- users" computers.

c) Warranty and Maintenance:

Computers purchased by College should preferably be with 1-year on-site comprehensive warranty. After the expiry of warranty, computers should be under the maintenance of RVS Maintenance Department. Department HODs should monitor for the proper and timely maintenance.

d) Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

e) Network Cable Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

f) File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

g) Non-compliance

Faculty, staff, and students of RVSCAS, who do not comply with this computer hardware installation policy, may leave themselves and others at risk of network related problems which could result in damaged or lost files and inoperable computers, resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, or even whole departments.

Hence it is critical to bring all computers into compliance as soon as they are recognized as non-compliant.

3. Software Installation and Licensing Policy

Any computer purchase made by the individual departments/projects should make sure that such computer systems have licensed software (such as operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, the College IT policy does not allow any pirated/unauthorized software installation on the college owned computers and the computers connected to the campus network. In case of any such instance, the department/individual shall personally be responsible for any pirated software installed on the computers located in their department/individuals' rooms.

Promoting Open Source Software

Free and Open Source Software (FOSS) Community is "By the Community, For the Community, of the Community, To the Community on No Profit No Loss Basis. Open Source Software, is and will always remain free. There is no license to pay to anybody." The central and state governments have introduced policies on the adoption of open source software, which make it mandatory for all software applications and services of the government built using open source software, so that projects under Digital India "ensure[s] efficiency, transparency and reliability of such services at affordable costs". The Government realizes that Free Software presents a unique opportunity in building a truly egalitarian knowledge society. RVS College encourages all members of its community to use FOSS to the extent possible. There is an immense opportunity to select and develop FOSS based on the requirements of the college.

a) Operating System and its Updation

1. Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through the Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS helps their computers in fixing bugs and vulnerabilities in the OS that are periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating the OS should be performed at least once in a week or so.

2. RVSCAS has made it a policy to encourage its user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.
3. Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is the users' responsibility to make sure that the updates are being done properly.

b) Antivirus Software and its updation

1. Computer systems used in the college have anti-virus software installed, and it is active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.
2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

c) Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer’s hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user’s data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data either on an external storage device or Google Drive for data integration.

d) Non-compliance

RVSCAS faculty (teaching & non-teaching) and students who are not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files, in-operable computer resulting in loss of productivity, risk of spread of infection to others or confidential data being revealed to unauthorized persons. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even the whole college. Hence it is critical to bring all computers into compliance as soon as they are recognized as non-compliant.

4. Network (Intranet and Internet) Use Policy

Network connectivity provided through an authenticated network access connection or Wi-Fi is governed under the College IT Policy. The RVS Infotech is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the College network should be reported to RVS Infotech.

a) IP Address Allocation

Any computer (PC/Server) that is connected to the college network should have an IP address assigned by the RVS Infotech. Departments should follow a systematic approach, the range of IP addresses that will be allocated to each building as decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer is connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location. As and when a new computer is installed in any location, the concerned user has to take IP address allocation from RVS Infotech / respective department. An IP address allocated for 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. IP addresses are given to the computers but not to the ports.

b) Proxy Configuration by Individual Departments /Cells/ Users

Configuration of proxy servers should also be avoided, as it may interfere with the service run by RVS Infotech. Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

c) Running Network Services on the Servers

Individual departments/individuals connecting to the college network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the RVS Infotech in writing and after meeting the requirements of the college IT policy for running such services. Non-compliance with this policy is a direct violation of the college IT policy, and will result in termination of their connection to the Network.

RVS Infotech takes no responsibility for the content of machines connected to the Network, regardless of those machines being College or personal property. RVS Infotech will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance. College network and computer resources are not to be used for personal /commercial purposes. Network traffic will be monitored for security and for performance reasons at RVS Infotech. Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

5. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty members (teaching & non-teaching) and students, and the College's administrators, it is recommended to utilize the College’s e-mail services, for formal College communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal College communications are official notices from the College to faculty members (teaching & non-teaching) and students. These communications may include administrative content, such as human resources information, policy messages, general College messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Faculty may use the email facility by logging on to https://gmail.com with their User ID and password. For obtaining the College’s email account, user may contact RVS Infotech for e-mail account and default password by submitting a request.

Users may be aware that by using the e-mail facility, the users agree 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 College'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 Page 13 of 30 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 e-mail account with others, as the individual account holder is personally held accountable, in case of any misuse of that e-mail account.
- While using the computers that are shared by other users as well, any e-mail 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 e-mail account of others will be taken as a serious offence under the College IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from the violations of College's e-mail usage policy.

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

6. Web Site Hosting Policy

a) Official Pages

Departments, Cells, central facilities may have pages on RVSCAS official Website. As on date, the RVS Infotech is responsible for maintaining the official website of the college viz., https://rvscas.ac.in/

b) Responsibilities for updating Web Pages

Departments are responsible to update their current information time to time about their web pages through their separate user login. Apart from that the web admin is responsible for update of the home page and other important pages. Major modifications on the structure and other things will be taken care by RVS Infotech.

7. College Database Use Policy

This Policy relates to the databases maintained by the College. Data is a vital and important College resource for providing useful information. Its use must be protected even when the data may not be confidential. RVSCAS has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the College's approach to access and use of this College resource.

Database Ownership: RVSCAS is the data owner of the entire College's institutional data generated in the College.

Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department.

MIS Components: Requirements for the purpose of Management Information System are:

- ❖ Employee Information Management System
- ❖ Students Information Management System
- ❖ Financial Information Management System
- ❖ Library Management System
- ❖ Document Management & Information Retrieval System

Here are some general policy guidelines and parameters for departments, cells and administrative department data users

1. The College's data policies do not allow the distribution of data that is identifiable to a person outside the College.
2. Data from the College's Database including data collected by departments or individual faculty and staff, is for internal College purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the College makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office.
5. Requests for information from any courts, attorneys, etc. are handled by the Office and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for response.
6. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes:
    - ❖ Modifying/deleting the data items or software components by using illegal access methods.
    - ❖ Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/departments.
    - ❖ Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
    - ❖ Trying to break security of the Database servers.

Such data tampering actions by College member or outside members will result in disciplinary action against the offender by the College authorities. If the matter involves illegal action, law enforcement agencies may become involved.

8. Wi-Fi Use Policy

- Usage of Wireless infrastructure is to enhance the accessibility of internet for academic purposes and to browse exclusive online resource (licensed online journals) of the RVSCAS for the students and faculty members.

- Availability of the signal will vary from place to place. The signal strength also may vary from location to location. It is not mandatory that each and every area in each floor of every block will have the same kind of signal strength, coverage and throughput.
- Access to Wireless internet is only an extended service and neither students nor anyone who is in the campus can demand the service. Availability of wireless services solely depends on the discretion of the RVSCAS and it has the rights to stop/interrupt the services at any given point of time, if required for any technical purpose.
- The access points provided in the campus are the property of RVSCAS and any damage or loss of the equipment will be considered as a serious breach of RVSCAS's code of conduct. Disciplinary action will be initiated on the students who are found guilty for the loss or damage of the Wireless Infrastructure or the corresponding equipment. In the incident of any loss or damage to the wireless infrastructure, RVSCAS will assess the damage and the same will be recovered from all the students who are residing in that floor/building.

9. Responsibilities of RVS Infotech

a) Campus Network Backbone Operations

- ❖ The campus network backbone and its active components are administered, maintained and controlled by RVS Infotech.
- ❖ RVS Infotech operates the campus network backbone in such a way that service levels are maintained as required by the College Departments, and hostels served by the campus network backbone within the constraints of operational best practices.

b) Maintenance of Computer Hardware & Peripherals

RVS Infotech is responsible for the maintenance of the College owned computer systems and peripherals that are under warranty or out of the warranty.

c) Receiving Complaints

The designated person in RVS Infotech receives complaints from the users of computer systems and coordinates with the service engineers of the respective brands of the computer systems (which are in warranty) to resolve the problem within a reasonable time limit. For out of warranty computer systems, problems are resolved by RVS Infotech.

RVS Infotech may receive complaints from department/users, if any of the networks related problems are noticed by them such complaints should be made by e-mail/phone.

RVS Infotech may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through a phone call.

The designated person in RVS Infotech receives complaints from the users and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

d) Scope of Service

RVS Infotech will be responsible for solving the hardware related problems or OS or any other application software that was legally purchased by the College and was loaded by the company as well as network related problems or services related to the network.

e) Installation of Un-authorized Software

RVS Infotech or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

f) Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of RVS Infotech.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of RVS Infotech. It essentially means exactly at which location the fiber optic based backbone terminates in the buildings and will be decided by the RVS Infotech. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of RVS Infotech.

3. RVS Infotech will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
4. It is not the policy of the College to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the College's Internet links.

g) Network Expansion

Major network expansion is also the responsibility of RVS Infotech. Every 3 to 5 years, RVS Infotech reviews the existing networking facilities, and need for possible expansion.

h) Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations RVS Infotech considers providing network connection through wireless connectivity.
2. RVS Infotech is authorized to consider the applications of Departments, or divisions for the use of radio spectrum from RVS Infotech prior to implementation of wireless local area networks.
3. RVS Infotech is authorized to restrict network access to the Cells, departments, or hostels through wireless local area networks either via authentication or MAC/IP address restrictions.

i) Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

j) Global Naming & IP Addressing

RVS Infotech is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. RVS Infotech monitors the network to ensure that such services are used properly.

k) Providing Net Access IDs and e-mail Accounts

RVS Infotech provides Net Access IDs and e-mail accounts to the individual users to enable them to use the campus-wide network and e-mail facilities provided by the College upon receiving the requests from the departments concerned.

l) Disconnect Authorization

RVS Infotech will be constrained to disconnect any Department, or cell, hostel from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Department, or cell, hostel machine or network, RVS Infotech endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Department or division is disconnected, RVS Infotech provides the conditions that must be met to be reconnected.

10. Responsibilities of Department

a) User Account

Any department, or cell or other entity can connect to the College network using a legitimate user account (Net Access / Captive Portal ID) for the purposes of verification of affiliation with the College. The user account will be provided by RVS Infotech, upon filling up the prescribed application form and submitting it to RVS Infotech.

Once a user account is allocated for accessing the College's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the College for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for e-mail account ID to prevent un-authorized use of their user account by others.

It is the duty of the user to know the IT policy of the College and follow the guidelines to make proper use of the College's technology and information resources.

b) Supply of Information by Department, or Cell for Publishing on/updating the RVSCASE Website

All Departments or Cells should provide updated information concerning them periodically (at least once in a month or earlier).

Hardcopy or softcopy to be sent to the RVS Infotech. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Department, or Cells.

Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the RVS Infotech upon receiving the written requests. If such web pages have to be directly added into the official web site of the College, necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the In Charge, RVS Infotech well in advance.

c) Security

In connecting to the network backbone, department agrees to abide by this Network Usage Policy under the College IT Security Policy. Any network security incidents are resolved by co-ordination with a Point of Contact (POC) in the originating department. If a POC is not available to contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/POC.

d) Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the College are the property of the College and are maintained by RVS Infotech and respective departments. Tampering of these items by the department or individual user comes under the violation of IT policy.

e) Additions to the Existing Network

Any addition to the existing network done by department or individual user should strictly adhere to the College network policy and with prior permission from the competent authority and information to RVS Infotech.

College Network policy requires following procedures to be followed for any network expansions:

1. All the internal network cabling should be as on date of CAT 6 UTP.

2. UTP cabling should follow structured cabling standards. No loose and dangling UTP cables are drawn to connect to the network.
3. UTP cables should be properly terminated at both ends following the structured cabling standards.
4. Only managed switches should be used. Such management module should be web enabled. Managed switches give the facility of managing them through web so that RVS Infotech can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.
5. As managed switches require IP address allocation, the same can be obtained from RVS Infotech on request.

f) Enforcement

RVS Infotech periodically scans the College network for provisos set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.

11. Responsibilities of the Administrative

RVS Infotech needs latest information from the different Administrative Departments for providing network and other IT facilities to the new members of the College and for withdrawal of these facilities from those who are leaving the College, and also for keeping the RVSCAS website up-to-date in respect of its contents.

The information that is required could be broadly of the following nature:

- ❖ Information about New Appointments
- ❖ Information about Termination of Services
- ❖ Information of New Enrolments
- ❖ Information on Expiry of Studentship/Removal of Names from the Rolls
- ❖ Information on Important Events/ Achievements
- ❖ Information on different Rules, Procedures, and Facilities

12. Guidelines for Those Running Application or Information Servers

Departments may run an application or information server. They are responsible for maintaining their own servers.

1. Obtain an IP address from RVS Infotech to be used on the server.
2. Get the hostname of the server entered in the DNS server for IP Address resolution
3. Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.
4. Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.
5. Operating System and the other security software should be periodically updated.

13. Guidelines for Desktop Users

These guidelines are meant for all members of the RVSCAS Network User. Due to the increase in hacker activity on campus, College IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1. All desktop computers should have the latest version of antivirus. And should retain the setting that schedules regular updates of virus definitions from the central server.
2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.
3. The password should be difficult to break.
4. The guest account should be disabled.

5. In addition to the above suggestions, RVS Infotech recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

14. Video Surveillance Policy

The system comprises: Fixed position cameras; Monitors; digital video recorders; Storage; Public information signs.

Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

a) Purpose of the system

The system has been installed by College with the primary purpose of reducing the threat of crime generally, protecting Colleges premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- ❖ Deter those having criminal intent
- ❖ Assist in the prevention and detection of crime
- ❖ Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- ❖ Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

It is recognized that members of College and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the RVS Infotech.