



JSS College for Women (Autonomous)

Saraswathipuram, Mysuru-570009

IT Policies & Guidelines

Table of Contents

Sl. No.	Chapter	Page Number
1	Need for IT Policy	3
2	IT Hardware Installation Policy	6
3	Software Installation & Licensing Policy	7
4	Network (Intranet & Internet) Use Policy	8
5	Web Site Hosting Policy	8
6	Responsibilities of Departments	8
7	Guidelines for Desktop Users	9
8	Video Surveillance Policy	10
9	Cyber Security	11
	Appendices	
1	Requisition Form for CCTV Footage	14

1. Need for IT Policy

- IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, Staff, Management and visiting Guests and Research Fellowship Members.
- Due to the policy initiative and academic drives, IT resource utilization in the Campus has grown by leaps and bounds during the last decade.

JSSCW has network connections for **249** Systems in College campus and **6** Systems in Hostel covering two buildings across the campus.

Computer Science is the department that has been given the responsibility of running the institute's Internet services.

JSSCW is getting Internet bandwidth of 10mbps broadband from BSNL, 20 mbps Leased Line from YashTel and 100mbps SME Line from YashTel total Internet Bandwidth of 130mbps in College Campus and 20mbps Broadband from BSNL in Hostel.

- When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users, who are on the high-speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network.

Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe download, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network.

They can slow down or even bring the network to a halt.

Containing a virus once it spreads through the network is not an easy job. Plenty of manheurs and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial.

Hence, in order to securing the network, Computer Center has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users.

As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions.

Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires.

Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

It may be noted that institute IT Policy applies to technology administered by the institute centrally or by the individual departments, to information services provided by the institute administration, or by the individual departments, or by individuals of the institute community, or by authorized resident or non-resident visitors on their own hardware connected to the institute network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centres, Laboratories, Offices of the institute, or hostels and guest houses, or residences wherever the network facility was provided by the institute.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the Institute's information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by the institute by any institute member may even result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

- Stake holders on campus
- Students: UG, PG, Research
- Employees (Permanent/ Temporary/ Contractual)
- Faculty
- 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

Policy Objectives: -

The objectives of the IT policy are as follows:

- To provide all required IT resources as per the academic programs also, introduce new IT technologies which will benefit the students and research staff.
- To effectively have an annual plan of introducing new technologies in-line with the Academia.
- Create provision for priority up-gradation of the products
- Create Provision for Annual Maintenance expenses to ensure maximum uptime of the products.
- Plan and invest for redundancy at all levels.
- To ensure that the products are updated and catered 24x7 in the campus or as per the policies lay down by the College Management.
- Leveraging information technology as a tool for the socio-economic development of the Institute.

2. IT Hardware Installation Policy

Institute network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she 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) 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 earthing and have properly laid electrical wiring.

c) 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.

d) 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.

e) Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the institute centrally will attend the complaints related to any maintenance related problems.

f) Noncompliance

JSSCW staff and students not complying 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, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

3. Software Installation and Licensing Policy

Any computer purchases made by the individual departments/cells should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

a) Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them.

b) Antivirus Software and its updating

Computer systems used in the institute should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

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 many volumes typically C, D and so on. OS and other software should be on C drive and user's data files on the other drives (e.g. D, E). 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 on CD / DVD or other storage devices such as pen drives, external hard drives.

4. Network (Intranet & Internet) Use Policy

Network connectivity provided through an authenticated network access connection or WiFi is governed under the Institute IT Policy. The Computer Science Department is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to Computer Science Department.

5. Web Site Hosting Policy

a) Official Pages

Departments, Cells, central facilities may have pages on JSSCW's official Web Site.

As on date, the Computer Science Department is responsible for maintaining the official web site of the institute viz., <http://www.jsscw.in>.

b) Responsibilities for updating Web Pages

Departments, cell, and individuals are responsible to send updated information time to time about their Web pages to Computer Science Department through Principal of the institution.

6. Responsibilities of Department

a) Supply of Information by Department, or Cell for Publishing on /updating the JSSCW Web Site

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 Computer Science Department. 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 Computer Science department upon receiving the written requests. If such web pages have to be directly added into the official web site of the institute, 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, Computer Science Department well in advance.

b) 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 institute are the property of the institute and are maintained by respective departments.

Tampering of these items by the department or individual user comes under violation of IT policy.

7. Guidelines for Desktop Users

These guidelines are meant for all members of the JSSCW Network User.

Institute 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.
- 3) The password should be difficult to break.
- 4) The guest account should be disabled.
- 5) In addition to the above suggestions, backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

8. 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.

❖ Purpose of the system

The system has been installed by institute with the primary purpose of reducing the threat of crime generally, protecting institutes 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.

CCTV footage provided by the institute upon receiving the requests from the individuals

9. Cyber Security

The JSSCW Management desires that its ITR (Information Technology Resources) be used in accordance with the College Code of Conduct and Policies and other regulations applicable from time to time by authorized users (AU). The College Management owns all the Technology Resources (TR) in the campus and holds absolute right over them.

- **Technology Resources (TR)** for the purpose of this policy include computer hardware, software and all allied services owned, operated or contracted by the college. These include all computer systems/devices such as desktop computers or multi-user systems whether free standing or connected to networks, laptops, printers, fax machines, cyclostyling machines, photocopiers, phones and other electronic devices; software, data, college email accounts, Wi-Fi and communication networks etc. associated with these systems.
- **Authorized Users (AU)** for the purpose of this policy include systems administrator, hardware/technical support team, students on the College attendance roll, faculty, administrative staff, multi-tasking staff and contractual staff.

The Right to Information Technology Resources provides reasonable access to TR. This privilege of access requires AU to act in an ethical manner and as a result imposes certain responsibilities and obligations. It is the responsibility of AU to respect the rights, privacy and intellectual property of others; respect the integrity of the resources; and abide by all local, state and national laws and regulations. Appropriate use of ITR by AU should always reflect academic honesty and good judgment in utilization of the shared resources and observe ethical, moral, and legal guidelines of the Management.

All ITR are the property of the College Management. The College's ownership of a file, record, data, or a message does not transfer ownership of any intellectual property therein. Incidental personal use is permitted as provided in this policy and is included in the definition of TR for the purposes of access and use. Records of electronic communications pertaining to the business of the teaching, learning, research, and administrative activities of the college are owned by the college.

The College Management holds the right to monitor, obtain access and ensure proper usage of ITR. Violation of this policy may result in disciplinary action up to and including rustication / suspension and cancellation of admission / contract and / or appointment in the College and in case of serious offences legal action.

The College may monitor the activity and accounts of users of ITR, with or without notice, when:

- It is necessary to protect the integrity, security, or smooth functioning of the college or other computing resources; or to protect the college from liability.
- There is reasonable cause to believe that the user has violated, or is this Information Technology Use Policy, other applicable college guidelines or policies or applicable laws or regulations.
- An account appears to be engaged in unusual or excessive activity, as indicated by the monitoring of general activity and usage patterns.
- It is otherwise required or permitted by law.

The College, at its discretion, may also disclose the results of such monitoring, including the contents and records of individual communications, to appropriate college personnel or law enforcement agencies, and may use those results in appropriate disciplinary proceedings.

The College management is sole owner of all the workplace accounts of all its employees and reserves complete and non-negotiable right of access to all of them.

Only AU may use College Technology Resource (CTR). AU of TR may be assigned one or more accounts with appropriate access restrictions. Individuals may only use TR to which they have been given access through an established college process.

Individuals User (IU) may not seek to change the permission associated with otherwise authorized accounts other than through approved processes by Technology Services (TS).

AU should use only those TR that they have been authorized to use, and only in the manner and to the extent so authorized. Users are responsible for any and all activity conducted with their login credentials.

Users of College Technology Resources (UCTR) shall not cause or attempt to cause, either directly or indirectly, excessive strain on any computing component or significant degradation of other users' ability on any college system, service or network resource.

UCTR shall not post unsolicited electronic mail to lists of individuals who have not requested membership in such list outside of a legitimate business purpose of the College. Nor shall users post obscene, harassing or otherwise inappropriate messages.

The college may take action to protect users from sending and / or receiving certain or all messages if they have a reasonable belief that such messages are the result of, or are causing, unauthorized interference with CTR or college operations.

UCTR must respect the privacy of others, and must protect the security, confidentiality, integrity and availability of information entrusted to them by the college.

UCTR must not inspect, disclose access, modify, render inaccessible or delete college data unless specifically authorized to do so.

UCTR may only use legally-obtained licensed tools and materials in compliance with the college laws and regulations.

TR may be used for limited personal purposes if such personal use does not:

- Directly or indirectly interfere with the college operation of computing facilities,
- Obligate the college in any business transaction or effort for any reason,
- Burden the college with noticeable incremental cost,
- Interfere with the computer user's employment or other obligations to the College,
- Violate other college policies, or applicable laws or regulations.
- Inconvenience other members of the college community
- Monopolize TR on the basis of rank, seniority or authority.

Appendix I

JSS College for Women (Autonomous)

Saraswathipuram, Mysuru-570009


Requisition for CCTV Footage

1. Name of Applicant : _____
2. Employee / Student Id : _____
3. Department : _____
4. Mobile No: _____
5. Email Mail Id : _____
6. Date of Footage : _____ Time : From _____ To _____
7. Camera Location : _____
8. Description : _____

Date:

.....

Signature of Applicant:


Principal
JSS College For Women (Autonomous)
Saraswathipuram, Mysuru-570 009