IT POLICY

Shailabala Women's Autonomous College
Cuttack-1

INFORMATION TECHNOLOGY INFRASTRUCTURE USAGE POLICY

Introduction

Students, Teaching and Non - Teaching Staff, Management and visiting Guests/faculties, Research Fellowship Members of Shailabala Women's Autonomous College availing computing, networking, and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system and protect the privacy and work of students and faculty.

General Rules

1. Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members are authorized to use the computing, networking, and other IT facilities for academic purposes, official business, and for personal purposes as long as such use does not violate any law or any college and government policy.

2. The College prohibits its users from gaining or enabling unauthorized access to forbidden IT resource on the college network. Any such attempt will not only be the violation of college Policy but may also violate national and international cyber laws, provisions under The Information Technology Act of India and infringe the principals of National Cyber Security Policy, and subject the user to both civil and criminal liability. However, the college reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own or through its affiliates.

3. The college prohibits its users from sending, viewing or downloading fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or college policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g. when such content is received through e-Mail etc. As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

4. Users must not violate various IPR and copyright law(s), and licensing policies as associated with copyrighted materials and software. Any unlawful file- sharing, use of any form of illegal or pirated or un-licensed software, on the college's IT resources (including individually owned IT resource being used under Institutional IT privileges) is strictly prohibited and any such act shall constitute a violation of the college policy.

5. College also recommends its students, faculty and office staff, to use Open Source Operating Systems (OS) and Processing Software (PS) such as Ubuntu/ CentOS or other and Libra Office/ Open Office/ WPS Office, respectively. Further, users of the computers sponsored directly or indirectly by Shailabala Women's Autonomous College may migrate on the recommended OS & PS as their primary software and should generate expertise on it. In case of technical limitation in such adaptation, relaxation may be requested from competent authority on valid grounds.

6. By agreeing to abide by the terms of use of various online media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, mailing lists, chat rooms, blogs, unless a user has proper authorization, no user should attempt to gain access to information and disclose the same to self or other unauthorized users. The broader concept of data privacy must be honored by each user.

7. No user should attempt to vandalize, damage or change any data inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resources must be preserved by all of its users. Any interference, disruption or encroachment in the college IT resources shall be a clear violation of the college policy.

8. No user should attempt to affect the availability of IT resource, whether accidently or deliberately.

9. As long as individual departments, Hostels, individual units etc. can retain consistency in compliance of the IT (Usage) Policy, the college, they may further define and implement additional "conditions of use" for IT resources under their control. It will be the responsibility of the Units to publicize and enforce such conditions of use. In cases where use of external networks is involved, suitable policies can be practiced in compliance with the broad prerogatives of (Usage) Policy of the college.

10. As a part of certain investigation procedures, the college may be required to provide its IT information, resource and/ or records, in parts or full, to third parties/ investigating agencies. Also, for proper monitoring and optimal utilization of college IT resources, the college may review, analyze and audit its information records, without any prior notice to its Users. Further, the college may also seek services from third-party service providers. Accordingly, the users can only have reasonable expectation of privacy on the college's IT resources.

11. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.

12. No food or drink is permitted in the laboratories. Also making noise either through games/music/movies or talking and/ or singing loudly (the list is not exhaustive) is prohibited.

13. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the college authorities may take an action.

14. The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the news groups.

2. College E-mail Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the College's administrators, it is recommended to utilize one well known registered 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, staff 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. Staffs, faculties and other employees can only send the email to the official email address of the college. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

2.1 The college email should be used primarily for academic and official purposes and to a limited extent for personal purposes.

2.2 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.

2.3 While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

2.4 The user(s) of the college email cannot pass the password or any sensitive information to anyone.

2.5 At the time of need of college e-mail for college works, any authorized employee can take the help of the Data Entry Operator or any authorized email operator who operates it. Certainly, he or she cannot take the password of the college email.

2.6 It is recommended in the policy to create an in-house college email based service for all the employees during the course of time.

3. Social Media Policy

POLICY

- This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include What's App, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others.

PROCEDURES

3.1 The following principles apply to professional use of social media on behalf of Shailabala Women's Autonomous College as well as personal use of social media when referencing the college.

3.2 Employees need to know and adhere when using social media in reference to College.

3.3 Employees should be aware of the effect their actions may have on their images, as well as the college's Image. The information that employees post or publish may be public information for a long time.

3.4 Employees should be aware that the College may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to the college, its employees, or customers.

3.5 Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment or which may hurt religious & Sentiments of any one or any Community.

3.6 Employees are not to publish post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the different Sections.

3.7 Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized College spokespersons.

3.8 If employees encounter a situation while using social media that threaten to become antagonistic, employees should disengage from the dialogue in a polite manner.

3.9 Employees should get appropriate permission before they refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

3.10 Social media use shouldn't interfere with employee's responsibilities at the College. The College's computer systems are to be used for the specific purposes only. When using college's computer systems, use of social media other than official purposes is not allowed. It is allowed only to those staff whose work profile requires use of social media (ex: Face book, Twitter, college's blogs and LinkedIn, What's app, Instagram, any other) , but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.

3.11 Subject to applicable law, after--hours online activity that violates or any other company/ govt. policy may subject an employee to disciplinary action or termination.

3.12 It is highly recommended that employees keep the college related social media accounts separate from personal accounts, if Possible.

3.13 Employees should not use any type of offensive /abusive language or make any comment/post any photo which is not in line with their image as a faculty/Teacher (As they belong to very respected community).

4. Responsibilities of Computer Centers, Laboratories, Departments, SAMS, Hostels etc.

A. Maintenance of Computer Hardware & Peripherals

The computers of the college will be maintained by the **Technical committee** irrespective of their possessing department. The **Technical committee** of the college is responsible for maintenance of the college owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Receiving Complaints

I. **Technical committee** may receive complaints from OICs/HODs/Co-ordinaotors/ Librarians/ Hostel Superintendents etc. through the Principal if any of the particular computer systems are causing any problem.

II. **Technical committee** may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them is having any problem.

III. The designated person(s) of **Technical committee** after receives complaints properly routed through Principal coordinates with the service engineers of the computer systems to resolve the problem within a reasonable time limit.

C. Scope of Service

Technical committee will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the College and was loaded by the authorized company.

D. Installation of Un-authorised Software

Technical committee or service engineers hired by them should not encourage installing any unauthorized software on the computer systems of the college. They should strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents

If members of the **Technical committee** or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the College, such incidents should be brought to the notice of the **Technical committee** and the College authorities.

F. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the **Technical committee**. After taking necessary corrective action **Technical committee** or service engineers should inform the concern OIC about the same, so that the port can be turned on by them.

G. Rebuilding the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net. Further, before reformatting the hard disk, (dump of only) the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

H. Coordination with Technical committee

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning **Technical committee/** service engineer may coordinate with the head or In-charge of the Concerned Unit (Library/SAMS/Hostels/Department) to resolve the problem with joint effort. This task should not be left to the individual user.

5. Guidelines for Desktop Users

These guidelines are meant for all members of the College/ users of the College Computers. To tackle the hacker activity on campus, The College IT Policy has put together the following recommendations to strengthen desktop security.

5.1 All desktop computers should have the latest version of a standardized antivirus and should retain the setting that schedules regular updates of virus definitions from the central server.

5.2 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.

5.3 All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.

5.4 The password should be difficult to break. Password, defined as:

i. must be minimum of 6-8 characters in length
ii. must include punctuation such as ! $ % & * , . ? + - =
iii. must start and end with letters
iv. must not include the characters # @ ' " `
v. must be new, not used before
vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.

5.5 Passwords should be changed periodically and also when suspected that it is known to others. Never use 'NOPASS', 'PASSWORD' etc. as your password.

5.6 Do not leave password blank and Make it a point to change default passwords given by the software at the time of installation.

5.7 The password for the user login should follow the same parameters outlined above.

5.8 The guest account should be disabled.

5.9 New machines with preloaded OS should activate the built-in firewall.

5.10 All users should consider use of a personal firewall that generally comes along the Anti-virus software, if the OS does not have an in-built firewall.

5.11 All the software on the compromised computer systems should be re-installed from scratch.

5.12 Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary

5.13 In general, start from a position of security that is most secure (i.e. no shares, no guest access etc.) and open up services as necessary.

5.14 In addition to the above suggestions, **Technical committee** 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.

5.15 Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

5.16 If a machine is compromised, immediately shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.

5.17 For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, the technical personnel of the department can scan the servers for vulnerabilities upon request.

6. Video Surveillance Policy

The system

6.1 The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: digital recorders; DVR/NVR Storage; Public information signs.

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

6.3 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/IP Camera installation is in use.

6.4 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 the College with the primary purpose of reducing the threat of crime generally, protecting college 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:

I. Deter those having criminal intent
II. Assist in the prevention and detection of crime
III. Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
IV. 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.
V. In the case of security staff to provide management information relating to employee compliance with contracts of employment

The system will not be used:

I. To provide recorded images for the world-wide-web.
II. To record sound other than in accordance with the policy on covert recording.
III. For any automated decision taking.

Covert recording

Covert cameras may be used under the following circumstances on the written authorization or request of the Principal or Administrative Bursar and where it has been assessed by the **Technical committee**.

I. That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
II. That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

III. Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.

IV. The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

7. Complaints

It is recognized that members of the College and others may have concerns or complaints about the operation of the system. Any complaint should be addressed to the Principal in writing. The **Technical committee** will look in to the matter and try to resolve within a stipulated time.