Kandivli Education Society's

B. K. SHROFF COLLEGE OF ARTS & M. H. SHROFF COLLEGE OF COMMERCE

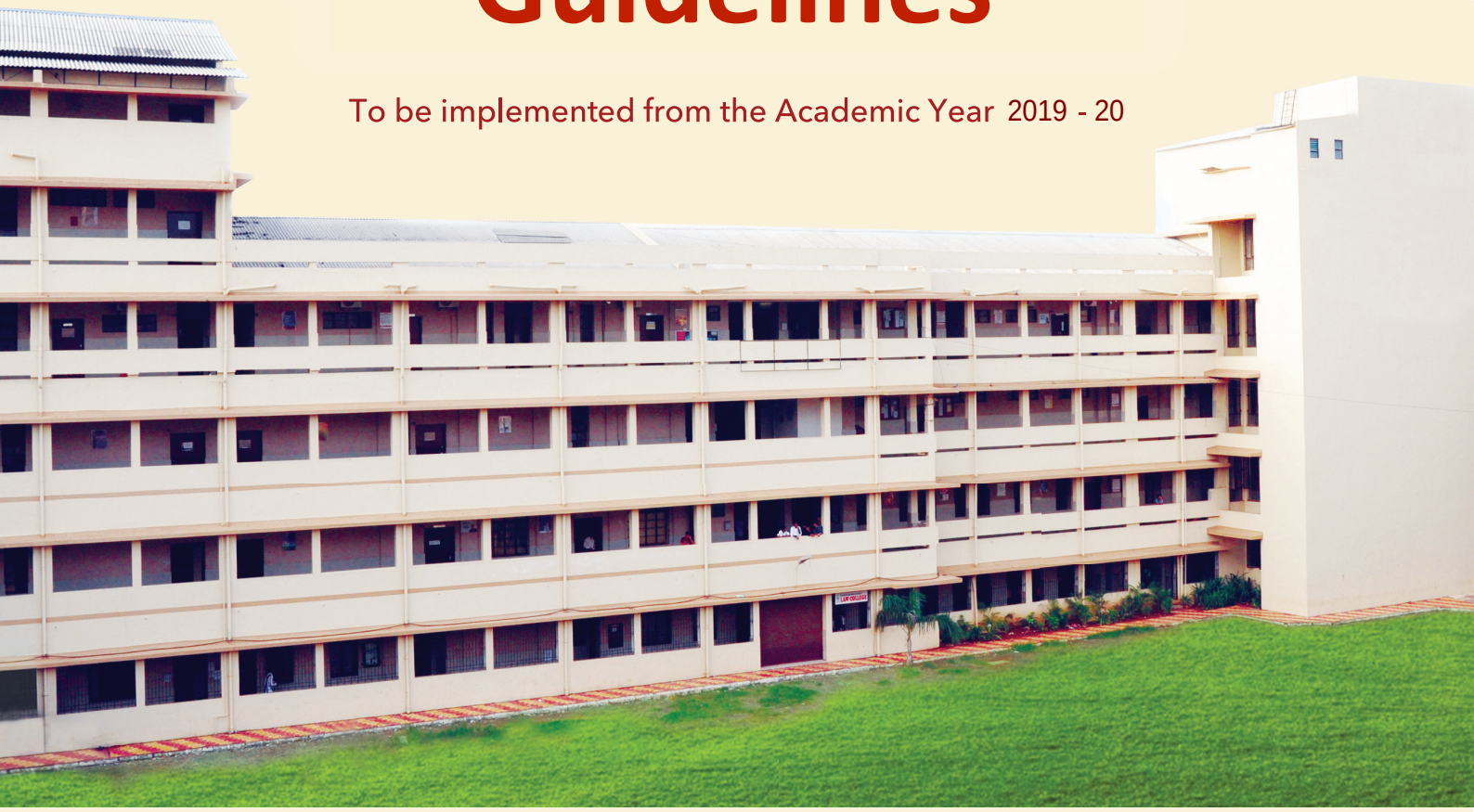
An Autonomous College

NAAC Re-accredited 'A' Grade | ISO 9001 : 2015 Certified

'Best College 2017-18' award from University of Mumbai

IT Policies & Guidelines

To be implemented from the Academic Year 2019 - 20



Bhulabhai Desai Road, Kandivali (West), Mumbai - 400067 | Tel.: 022 - 28053104
Cell : 9920235062 | Email : kessc1989@gmail.com | Website : www.kesshroffcollege.com

IT Policies & Guidelines

Prepared by

Department of Information Technology ,

KES Shroff College ,

Mumbai, 400067.

Table of Contents

KES Shroff College (Autonomous)

IT Policy

1. Need for IT Policy

The Information Technology (IT) Policy of the organization defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the employees pertaining to technological assets and services used for office work. This policy establishes strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the College.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information. The IT policy of institution

Applies to

a. Stake holders on campus and off campus
b. Students: UG, PG, Research
c. Employees(Permanent/ Temporary/ Contractual Faculty)
d. Administrative Staff (Non-Technical / Technical)
e. Higher Authorities and Officers

Resources

a. Network Devices wired/ wireless Internet Access
b. Official Websites, web applications
c. Official Email services
d. Data Storage

e. Mobile/ Desktop /Laptops / Server computing facility
f. Projectors, Smartboards
g. Documentation facility (Printers/Scanners)
h. Multimedia Contents

The IT policy of KES Shroff College includes

Purchase:-

a. The Purchase Committee procedures & guidelines need to be followed to purchase new technological equipment, services or software for official purposes.
b. All approved equipment, services or software will be purchased through the Purchase Committee, unless informed/permitted otherwise.
c. IT Dept. will assist the Purchase Committee while evaluating the best and the most cost-effective hardware or software to be purchased for a particular dept./project/purpose based on the requirement. The IT Dept. will also make sure all hardware/software standards defined in the IT Policy are enforced during such purchases.

Compliance:-

a. All employees are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the organization.
b. Any employee who notices misuse or improper use of equipment or software within the organization must inform his/her Head of Department immediately.
c. Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the authority.

Employee Training :-

a. Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software.
b. Employees can request and/or the IT Coordinator or Management can decide to conduct an IT training on a regular or requirement basis.

IT Support:-

a. IT support in the college is provided by Department of Information Technology.
b. For any technical help required by any employee the IT department teachers provides support. same the AMC service provider is to be called and should and they resolve the issue.
c. The college has appointed external agency for Hardware support and maintenance.
d. Tickets will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the designated team in IT Dept.

IT Hardware Installation Policy

College 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. **Who is 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. **Warranty & Annual Maintenance Contract**

Computers purchased by any Section/Department/Project should preferably be with 1-year on- site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include Operating System (OS) re-installation and checking virus related problems also.

c. **Power Connection to Computers and Peripherals**

All the computers and peripherals should be connected to the electrical point through UPS if possible. 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.

d. **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.

e. **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.

f. **Shifting Computer from One Location to another**

Computer system may be moved from one location to another with prior written intimation to the IT Dept., as IT Dept. maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified . When the end user meets the compliance and informs IT Dept. in writing/by email, connection will be restored.

g. **Maintenance of Computer Systems provided by the College**

For all the computers that were purchased by the College centrally and distributed by College AMC service provider will attend the complaints related to any maintenance related problems.

Software Installation and Licensing Policy

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

A. Operating System and its Updation

1. 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. 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. Checking for updates and updating of the OS should be performed at least once in a week or so.
2. College as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

B. Antivirus Software and its Updation

1. Computer systems used in the College 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.
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 storage devices like pen drive and external hard disk.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the College, referred to hereafter as "The Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the College IT Policy. The AMC service provider is responsible for the ongoing maintenance and support of the Network, exclusive of local applications.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the College network, should have an IP address assigned by the IT Dept. Following a systematic approach, the range of IP addresses that will be allocated to each building is 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 will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorizedly from any other location.

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. Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any Section, department of the College under any research programme/project should ideally be pooled with the College's Internet bandwidth, and be treated as College's common resource.

Under particular circumstances, which prevent any such pooling with the College Internet bandwidth, such network should be totally separated from the College's campus network. All the computer systems using that network should have separate IP address scheme and the College gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the College IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to IT Dept..

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff 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, staff and students. These communications may include administrative content, such as human resources information, policy messages, general College messages, official announcements, etc.

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

1. the facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
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.
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.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. 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.

6. Users should configure messaging software on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
7. 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.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. 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.
10. Impersonating email account of others will be taken as a serious offence under the College IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of College's email usage

.

College Database (e-Governance) Use Policy

This Policy relates to the databases maintained by the College administration under the College's e-Governance. 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. KESSC 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 both the access and use of this College resource.

1. **Database Ownership:** KES Shroff College is the data owner of all the College's institutional data generated in the College.
2. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute College's database. They may have custodianship responsibilities for portions of that data.
3. **Data Administrators:** Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

Here are some general policy guidelines and parameters for Sections, departments and administrative unit 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. 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 College Principal.
4. Requests for information from any courts, attorneys, etc. are handled by the Dean of Administration of the College and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the College for response.
5. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Dean of Administration/Controller of Examinations.

6. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to :
    a. Modifying/deleting the data items or software components by using illegal access methods.
    b. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
    c. Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
    d. 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

Video Surveillance Policy

The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors, Servers, Multiplexers; digital recorders; SAN/NAS 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/IP Camera installation is in use.

Purpose of the system

The system has been installed by College with the primary purpose of reducing the threat of crime generally, protecting college premise and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy.

The system will not be used:

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

The Security Control Room

Images captured by the system will be recorded in the Security Control Room, "the Server room", twenty-four hours a day throughout the whole year. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry.. Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Principal. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.

Recording

Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time. Images/videos will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly. All hard drives and recorders shall remain the property of College until disposal and destruction.

Access to images

All access to images/videos will be recorded in the Access Log as specified in the Procedures Manual. Access to images/videos will be restricted to those staff need to have access in accordance with the purposes of the system after permission from the Principal.

Access to images by third parties

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities only after permission from the Principal :

1. Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
2. Prosecution agencies
3. Relevant legal representatives
4. The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
5. People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
6. Emergency services in connection with the investigation of an accident.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Principal. Principal has all rights to refuse the application.