M.K.E.S. COLLEGE OF LAW

INFORMATION TECHNOLOGY POLICY

V. R. Dube

DR.VANDANA R.DUBE

I/c PRINCIPAL

SHRI DIGANT H.UPADHYAYA

HON.SECRETARY

M.K.E.S. College of Law

IT POLICY

Introduction

M.K.E.S. College of Law IT Policy and Procedure Manual provides the policies and procedures for selection and use of information technology within the institution, which must be followed by all staff and students. It also provides the guidelines that M.K.E.S. College of Law will use to administer these policies, with the correct procedure to follow. M.K.E.S. College of Law will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome. These policies and procedures apply to all employees and learners.

Objectives

The objectives of IT policy of M.K.E.S. College of Law are:

1. to provide and maintain technological products, services and facilities like Personal Computers (PCs), peripheral equipment, servers, telephones, Internet and application software to its employees and students for official and academic use.
2. to define 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.
3. To provide guidelines for issues like purchase, compliance, IT support and grievance redressal of the employees and students pertaining to technological assets and services used for office work.

IT Infrastructure of the Organization:

The term IT covers the following areas of M.K.E.S. College of Law:

1. Technology and hardware
2. Software
3. Data and network Security
4. IT infrastructure administration
5. Website

6. Equipment usage and maintenance
7. Emergency Management
8. Online content usage

Purchase, Implementation, Usage and Maintenance of IT Infrastructure

Policy covers the following vast areas:

1. Policy for the Purchase of Hardware

This policy provides guidelines for the purchase of hardware for the institution to ensure that all hardware technology for the institution is appropriate, value for money and where applicable integrates with other technology for the institution. The objective of this policy is to ensure that there is minimum diversity of hardware within the institution. The following guidelines exist for the purchase of hardware.

a. All the hardware purchase should be done by the purchase committee in consultation with the management.
b. According to the requirement submitted by the concerned staff or Department, the quotation is called for and after meeting with the parties, the order is placed.
c. Warranty and supporting documentations are to be preserved by the IT Administrator.

2. Policy for the procurement and usage of Software

Procurement policy provides guidelines for the purchase of software for the institution to ensure that all software used by the institution is appropriate, value for money and where applicable integrates with other technology for the institution. This policy applies to software obtained as part of hardware bundle or pre-loaded software. Usage policy provides guidelines for the use of software for all employees and students within the institution to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

The purchase of all software must adhere to this policy.

a. All software, including commercial or non-commercial software must be approved by IT Administrator prior to the use or download of such software.
b. All purchased software must be purchased by M.K.E.S. College of Law.

c. All purchases of software must be compatible with the institution's server and/or hardware system. Any changes from the above requirements must be authorised by the IT administrator and Principal.

d. Open source or freeware software can be obtained without payment and usually downloaded directly from the internet. In the event that open source or freeware software is required, approval from IT administrator must be obtained prior to the download or use of such software. All open source or freeware must be compatible with the institution's hardware and software systems.

e. All computer software copyrights and terms of all software licences will be followed by all employees and students of the institution. Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of IT administrator to ensure these terms are followed.

f. IT administrator is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and licence agreements are adhered to.

g. All software must be appropriately registered with the supplier where this is a requirement. M.K.E.S. College of Law is to be the registered owner of all software.

h. Only software obtained in accordance with the getting software policy is to be installed on the institution's computers.

i. All software installation is to be carried out by the lab technical staff.

j. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

k. Only software purchased in accordance with the getting software policy is to be used within the institution.

l. Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

m. All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of the IT administrator.

n. Employees and students are prohibited from bringing software from home and loading it onto the institution's computer hardware. Unless express approval from the Principal is obtained, software cannot be taken home and loaded on anybody's home computer.

o. Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from the IT administrator and Principal is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the institution and must be recorded on the software register by the IT administrator.

p. Unauthorised software is prohibited from being used in the institution. This includes the use of software owned by an employee and used within the institution.

q. The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to the Principal and strict disciplinary action will be taken.

r. Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Principal immediately.

3. IT Security Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the institution to ensure integrity, confidentiality and availability of data and assets.

a. For all servers and other network assets, the area must be secured with adequate ventilation and appropriate access through keypad, lock etc.

b. It will be the responsibility of the IT administrator to ensure that this requirement is followed at all times.

c. Any employee becoming aware of a breach to this security requirement is obliged to notify the Principal immediately.

d. All security and safety of all portable technology, will be the responsibility of the employee who has been issued with it.
e. All critical institutional data should be backed up.
f. It is the responsibility of IT administrator to ensure that data back-ups are conducted regularly and the backed up data is kept securely.
g. All technology that has internet access must have anti-virus software installed. It is the responsibility of IT administrator to install all anti-virus software and ensure that this software remains up to date on all technology used by the institution. All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements. Strict disciplinary action will be taken against any employee or user breaching this.
h. Every employee, if required, will be issued with a unique identification code to access the institution technology and will be required to set a password for access.

4. IT Administration Policy

This policy provides guidelines for the administration of information technology assets and resources within the institution.

a. All software installed and the licence information must be registered on the office records.
b. IT administrator is responsible for the maintenance and management of all service agreements for the institution technology. Any service requirements must first be approved by IT administrator.
c. IT administrator is responsible for maintaining adequate technology spare parts and other requirements including toners, printing paper etc.
d. Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.
e. All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.
f. Default passwords on all systems must be changed after installation.

g. Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.
h. Virus prevention for personal computers and email usage has been described previously.
i. Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.
j. Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.
k. Intrusion detection must be implemented on all servers and workstations containing high and medium risk data.
l. Operating system and application software logging process must be enabled on all systems.
m. Server, firewall and critical system logs must be reviewed frequently.
n. A technology audit is to be conducted regularly by an expert to ensure that all information technology policies are being adhered to.
o. Any unspecified technology administration requirements should be directed to the Principal.

5. Website Policy

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

a. A website register must be there to record the following details: List of domain names registered to the institution, Dates of renewal for domain names, List of hosting service providers, Expiry dates of hosting, etc.
b. All content on the institution website is to be accurate, appropriate and current.
c. All content on the website must follow institution's content plan and guidelines.
d. The content of the website is to be reviewed.
e. Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the institution.

6. Equipment Usage, Maintenance and Security

a. It is the responsibility of all employees and students to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.

b. Proper guidelines or safety information must be obtained from designated staff before operating any equipment for the first time.

c. Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff.

d. Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.

e. If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from your IT administrator is required for the same. The malfunctioning device needs to be submitted to the IT technical staff for checking, maintenance or repair.

f. The IT administrator can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT staff. The issue will then be resolved by the IT administrator in consultation with the technical team. The Principal can be consulted in terms of serious disputes or unresolved issues.

7. Emergency Management of IT

This policy provides guidelines for emergency management of all information technology within the institution.

a. Where there is failure of any of the institution's hardware, this must be referred to IT administrator immediately. It is the responsibility of IT administrator to take the appropriate action in the event of IT hardware failure, in consultation with the Principal.

b. It is necessary to undertake tests on planned emergency procedures regularly to ensure that all planned emergency procedures are appropriate and minimise disruption to institution operations.

c. IT administrator is responsible for ensuring that any security breach is dealt with the fastest mode to minimise disruption to institution operations.

d. In the event that institution website is disrupted, the following actions must be immediately undertaken: Website host to be notified, Principal must be notified immediately and the necessary corrective measure is to be done as early as possible.

8. Online Content Usage Guidelines

a. Internet is a paid resource and therefore shall be used only for office work.

b. The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.

c. The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The Management Committee can choose to analyse Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.

d. The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.

e. Employees and students are solely responsible for the content accessed and downloaded using Internet facility in the office or computer lab or college premises. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.

f. During office hours, employees are expected not to spend time to access news, social media and other websites online, unless explicitly required for office work.

g. Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.

h. Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

9. Inappropriate Use

The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the Management Committee as deemed fit. Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

a. Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
b. Downloading images, videos and documents unless required to official work
c. Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work
d. Accessing pirated software, tools or data using the official network or systems
e. Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee
f. Engaging in any criminal or illegal activity or violating law
g. Invading privacy of co-workers
h. Using the Internet for personal financial gain or for conducting personal business
i. Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
j. Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation

~~~~~~~~
~~~~~~~~