K.L. MEHTA DAYANAND COLLEGE FOR WOMEN, FARIDABAD

IT Policy & Guidelines

K.L. Mehta Dayanand College for Women, Faridabad has taken a number of efforts to use information and communication technology to perform administrative tasks, financial management, online admissions, test-related tasks, library operations, services and teaching. A comprehensive College network was established in 2003. Since then, the use of ICT and network services has seen tremendous growth. As a result, College administrators see the need to develop an IT policy to ensure efficient use of IT resources and bandwidth; effective control over activities that take place in the College network, whether related to the College or not and security of College-based IT resources. Users of network and computer resources are responsible for the proper use and protection of resources and also respect for the rights of others. All members of the College are expected to be familiar with and follow this policy.

Objectives of IT Policy

The objective of this policy is to ensure the protection of College's information technology resources from unintentional damage, unintentional access or damage while also preserving and nurturing the information-sharing requirements in its academic culture.

This policy is applicable to all staff, students and to all others granted use of K.L. Mehta Dayanand College for Women Faridabad, information resources. This policy refers to all College information technology resources controlled by management, stand-alone or networked resources. This includes all networked devices, including digital assistants, Cell phones, personal computers, workstations, minicomputers, other wireless devices and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

College is committed to ensure appropriate security for information technology systems in its ownership and control. College recognizes its responsibility to give awareness and security among the members of the College.

Each user of the College Information Resources must ensure that it is used for promoting the mission of the College towards teaching, learning, research, and administration. In particular, the major objectives of this document are:

A. To ensure the integrity, reliability, availability, and superior performance of the College IT Systems including smart boards.

B. To ensure that the IT resources protects the official e-identity (allocated by the College) of an individual.

C. To ensure that all the users of the College are responsible for adhering to the procedures governing the implementation of this Policy document and any other matter incidental to those rules.

IT for Governance

The entire administrative process will be computerized. Help desks will be built for College participants. Improved security systems, efficiency and transparency will be adjusted /

redesigned. IT will be used to monitor and manage College resources. IT will be used for grievance redress and remedial action. Staff development programs will be provided from time to time to develop the skills of College staff to use ICT.

IT Hardware Installation Policy

College system user group needs to notice certain provision while getting their computers or peripherals installed so that they may face minimum trouble due to involvement 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 her/him is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the college administrator should make an arrangement and make its compliance possible giving responsibility to a person.

B. Warranty & maintenance

Computers purchased by college should preferably have 3-year on-site comprehensive warranty and after the expiry of warranty, computers should be under computer hardware expert .Such maintenance should include Operating System 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 online UPS. Electricity supply to the UPS never be switched off, as continuous electricity supply to UPS is required to charge the battery. Further, these UPS systems should be connected to the socket that are provided with proper earthing and have properly laid electrical wiring.

D. Network Cable Connection

While connecting the computer to the network, the connected network cable should be away from any electronic equipment, as they interfere with the network communication. Further, no other electronic equipment should be shared with the power supply from where the computer and others 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 completely 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 location with earlier written intimation to the IT Cell, as IT Cell maintains a record of computer identification names and corresponding IP address. As and when any difference (from the list maintained by IT Cell) 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 Cell in writing/by email, connection will be restored.

G. Maintenance of Computer Systems provided by the College

For all the computers that are purchased by the College, IT Cell will attend the complaints related to any maintenance related problems.

Software Installation and Licensing Policy

Any computer purchases made by the College, such computer systems should have licensed software (operating system, antivirus software and necessary application software) installed.

College IT policy does not allow any pirated and unauthorized software to be installed 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 Updating

Individual users should make sure that respective computer systems have their OS updated in respective of their service pack, through Internet. This is particularly important for all MS Windows based computers .Checking for updates and updating of the OS should be performed at least once in a week or so.

B. Antivirus Software and its updating

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 the virus protection policy of the college.
2. Individual users should make sure that the individually computer systems have virus protection software installed and properly maintained.
3. He/she should make sure that the software is working correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after complete its warranty period, practically has no use. If these responsibilities appear beyond the end user's technical skills and the end-user is responsible for seeking assistance from any member of IT Cell.

C. Backups of Data

Computer users should perform regular backups of their important data. Virus may destroy the data on an individual's computer. Without proper backups, recovery of destroyed files may not be possible.

Preferably, at the time of Operating System installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D drive. OS and other software should be on C

drive and user's data files on the D drive. In case of any virus related problem, generally only C drive data 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 Google drive or other storage devices such as pen drives.

An individual's non-compliant computer can have significant, adverse effects on the other individuals, departments, or even whole College. Hence it is very difficult to bring all computers into compliance as soon as they are recognized not to be.

Procurement Policy

Computer hardware and software with standard definitions will be available for easy support and sharing of resources / information. Attempts will be made to last as long as possible warranty. After the expiry of the warranty period, some IT items such as CCTV camera, library software, tally software, payroll software, and firewall must be delivered under AMC cover. The terms and conditions of the AMC should be necessary for the maintenance of software. Software site licenses, as they are cheaper, should be purchased where possible. The user requirements of the computational power will be determined and met from the available resources. For asset management purposes, an inventory of all IT products will be conducted by each Department in consultation with the College IT Cell.

Installation Policy

1. In College, some persons will be appointed as the team responsible for IT policy and good governance.
2. Procurement of computers by individual departments, if available, will ensure that those computer programs are pre-loaded with licensed software - operating system, anti-virus software and required software.
3. IT Cell will be responsible for updating the OS with respect to the Internet service packages / shares. OS updates and software updates should be done at least once a week however.
4. The main user of the computer program is responsible for keeping the computer system compliant with this procurement policy.

Virus Protection Policy

This Policy supplements specific information about how the IT Cell, manages the potential risk of Virus infection. All systems and Files Servers will be protected by Anti-virus software. A member of IT Cell will install the latest version of the software in all systems. Departments that have received PCs that have not been taken to the IT Department for installation must ensure that an IT Technician loads the latest version of the Virus protection software onto the PC, Laptop or PDA. PCs will be updated automatically by the central software installation servers where

possible. The users will be shown how to update their virus protection software. Users requiring this arrangement must contact the IT Cell for further information. All removable media that will be used on PCs must first be virus scanned to ensure that there is no viruses' resident on the media. All E-mail attachments must first be virus scanned before opening, failure to do so could result in a major security incident. The IT Cell recommends that files only be downloaded from the internet if absolutely necessary. All the files downloaded from the internet must be virus scanned before to opening. The virus detection software is designed to start-up automatically when the PC starts up; this is to ensure that the PC is protected at all times. In the event that a virus is found or suspect on a user's PC, they should contact the IT Helpdesk immediately. The user must follow the instruction of the IT staff, which may involve ceasing all work on the PC and labeling it so that other people do not attempt to use it. The PC should be disconnected immediately if it is connected to the network. IT department will investigate the incident and will take any action to resolve the issue.

System & Network Use Policy

1. When connecting a computer to a network, the network cable should be away from any electrical equipment, as it interferes with network communication. As far as possible, no other electrical / electronic equipment should be shared with electrical power from a computer connection.
2. Access to remote networks using a College network connection must comply with all policies and rules of those networks. This applies to any networks to which a College network is connected.
3. Use of College network and computer equipment for commercial purposes is not permitted. Network jam will be monitored for security and performance reasons.
4. Impersonating an authorized user while connecting to a College network would be a violation of College IT policy. It will lead to termination of communication and will call for disciplinary action.

E-mail Account Use Policy

College staff will use the College's official email services for all official communications by logging into the College website (https://www.klmehtadcw.org) with their IT-Cell User ID and password. Employees will keep their email account active by using it regularly. Users should be aware that by using the email site, users agree to comply with the following policies:

1. The institution must be used for educational purposes.
2. Using the institution for illegal / commercial purposes is a violation of College IT policy. It will involve the withdrawal of the institution, with the exception of other disciplinary action. Illegal use includes unauthorized copying or distribution of software, sending unsolicited email messages, threatening, harassing, fraudulent messages / images or scams, and other similar acts.
3. While sending a large attachment to others, the user shall ensure that the recipient has an email address that allows him or her to receive such a large attachment.

4. User must keep the mailbox used within 80% usage, as 'mailbox is full' or 'mailbox almost full' will result in unsolicited emails, especially when incoming mail contains large attachments.
5. User must not open any email or attachments from an unknown and suspicious source. Even if it comes from a reputable source, and if it contains any suspicious or suspicious natural attachment, the user must obtain confirmation from the sender of its authenticity before opening it.
6. A user must not share his e-mail account with others, as each account holder is responsible for the misuse of that e-mail account.
7. While using computers shared by other users and, any email account left accidentally opened by another user, must be closed immediately without regard to the contents of it, by the user who has used that computer to use it.
8. Creating a personal email account for others will be considered a serious offense under the College IT policy. It will call for legal action against the perpetrator.

The policies outlined above especially 1 to 8 apply even more to email services provided by other sources such as Gmail.com, rediffmail.com, as long as they are used on a College network, or by using individual College-provided resources for official use even and outside.

Web Site Updating, Hosting & Maintenance Policy

A. Official Pages

I. The College's Website committee maintains the official web site of the College viz., https://www.klmehtadcw.org only.
II. The departments shall be responsible for the supply of information to IT-Cell in the form of a softcopy accompanied by a hardcopy. The information to be supplied by departments, offices includes advertisements, tender notifications published in newspapers, events organized/to be organized, admissions information and such other information as may be required to be uploaded on the web site. Such information will be uploaded on the College website by IT-Cell as early as possible.
iii. Official Web pages must confirm to the College Web Site Creation Guidelines for Website hosting.

B. Learning Management System i.e. e-Learning

Faculty may have class materials (syllabi, course materials, etc.) on the Web, linked through the appropriate pages in Learning Management System.

C. Policy for Maintaining Web Pages

a. Pages must relate to the University's mission.
b. Authors of official pages are required to announce their Web presence by sending an announcement to college official Mail-Id. The announcement should include the URL and a brief explanation of content or purpose of the pages (Web pages for an administrative or academic unit, etc.).

Responsibilities of Those Maintaining Web pages

Departments and Clubs/Cells are responsible for maintaining their own Web pages. All Web pages must adhere to the College Web Page design guidelines. Standards and Design Guidelines should be approved by IT-CELL/Committee constituted by the College for this purpose.

IT infrastructure and information security policy

A. **Security Policy**: The Principal of College will appoint a competent person to oversee the security of sensitive / confidential information stored in College programs and / or transmitted over the College data network. It will also look at the security of critical IT infrastructure. It will put in place appropriate policies and procedures in this regard, and monitor their implementation.

B. Infrastructure Division:

i. Key Infrastructure: Sensitive infrastructure includes data infrastructure (including data / data contained in it) and network core (Core switches, Zone switches (s), routers, incoming links from ISPs, fiber cable, etc.). This should be given the highest level of security through firewall protection. Any unauthorized national / international hacking / hacking will call for disciplinary action / prosecution.

ii. Essential Infrastructure: Distribution of network cable installation used to connect critical systems, development systems, systems used for e-governance activities, and project plans - programs used for modern operational purpose in various departments. This should be given significant security. Any unauthorized national / international hacking / hacking will call for disciplinary action / prosecution.

iii. **Needed Infrastructure:** Non-essential and essential infrastructure such as programs and networks in library. Any unauthorized access, hacking can lead to disciplinary action. Any unauthorized national / international hacking / hacking will call for disciplinary action / prosecution.

C. Physical Protection: Linear security will be put in place to protect College IT infrastructure.

D. Data classification and storage: Data will be categorized into security categories. Management practices will be put in place to ensure adequate security / privacy for each category. Data will be stored offline. Thereafter, it will be archived or terminated with prior approval by the appropriate authority.

Responsibilities of College IT Cell

A. Campus Network Backbone Maintenance

IT-Cell will be responsible for the management, maintenance and control of the campus network backbone and its operations.

B. Network Services Maintenance

IT-Cell will handle the operation networks and internet services. All network failures and overuse should be reported to IT-Cell to resolve issues.

Uninterrupted monitoring of the campus network fullness will be carried out by IT-Cell on a regular basis. If traffic patterns suggest that system or network security, integrity or network

performance are compromised, IT-Cell will review the traffic violations, identify equipment, and take security measures.

C. Physical connection of Campus buildings to Campus Network

i. IT-CELL will deal with the physical connection of campus structures to the backbone of the campus network.
ii. All buildings must have cable such as electrical and telephone cables. To ensure this, the hardware Expert will be responsible for taking all necessary steps.
iii. IT-Cell will consult with Management to ensure that the needs of end users are met while protecting the integrity of the backbone of the college network.

D. Network Renewal and Expansion

IT-Cell will review existing network structures every 2-3 years and take the necessary steps to upgrade / expand it.

E. Wireless Local Area Networks

i. When access to Fiber Optic / UTP cables is not possible, network communication will be provided via wireless technology.
ii. IT-Cell will be responsible for controlling network access to departments / facilities / offices through local wireless network either through authentication.
iii. Users (Staff or students) will make a written request to IT-Cell by providing internet access through Wi-Fi. Such a request must be recommended by the relevant Head of Department / Office. Thereafter, IT-Cell will assign the password to the applicant.
v. IT-Cell will keep a proper record of Wi-Fi user.

F. Electronic Logs

Electronic logs created as a result of network traffic monitoring may be retained until their administrative need is exhausted. Logs can be traced.

G. Global Naming & IP Addressing

IT-Cell will be responsible to provide a consistent forum for the allocation of campus network services such as IP addressing. IT-Cell will be monitored the network to ensure that such services are used properly.

H. Filing of Complaints by the Users

i. All network-related complaints will be filed with the IT-Cell.
ii. IT-Cell will attend such complaints as early as possible.
iii. IT-Cell will maintain a log of the complaints received and complaints attended.

I. Maintaining Digital library – Maintaining the digital library is also the responsibility of IT Cell. The Library is well equipped with automated software TECHLIB7 to streamline the data,

including functional modules such as circulation, acquisition, Cataloguing, serials management, flexible reporting, OPAC etc. and is switching towards KOHA library software. The college has also implemented the Web OPAC to facilitate the users to avail library services through internet. The college library has also subscribed to N-List programme of Inflibnet. Besides that, college has its own e-Library and students can read from peer reviewed journals, e-books, thesis from world class publishers. The college also uploads video lectures and presentations related to curriculum, on e-Library as Learning Management System (LMS).Library has its own computer center and internet connection is available for the students and teachers to access electronic resources.

J. Procedure of Redressal of IT Complaints

i. Every lab has one Maintenance Register for the systems in that lab.
ii. If there is some problem in any PC or Projector, then the allotted number of PC and the problem is written in register.
iii. The Admin Department appoints the problem to a hardware person.
iv. If problem is not resolve by the hardware person then outsourcing is done.
v. It is updated in Register.

Responsibilities of the Administrative Units

IT Cell needs the latest information from the various administrative structures of the College by providing network and other IT services to new College members and the withdrawal of these institutions from College leavers, as well as maintaining the KLMDN website - up to date on its content.
The information required can be as follows:
1. Details about new suspensions / promotions.
2. Details about Super annotations / Termination of Services.
3. Details of New Registration.
4. Details of the expiration date / deletion of words on the Rolls.
5. Any action by the College authorities that disqualifies an individual from using the College's network resources.
6. Details of important events / developments / achievements.

Guidelines for Desktop Users

These guidelines are meant for all members of the users of the College network.
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 such as Scan Anti-Virus or Quick Heal and should retain the setting that schedules regular updates of virus definitions from the systems.
2. When a desktop computer is installed, all operating system updates. In addition, operating system updates should be applied regularly, on an ongoing basis.

3. All Windows 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.
4. Password should be difficult to break. Password, defined as:

i. It should be at least 6-8 characters long
ii. It must include punctuation marks such as! $% & *,. ? + - =
iii. It should start and end with letters
iv. It must not enter characters # @ """
v. It should be new, not used before
vi. Avoid using your name, or the names of your wife or children, or the name of your department, or room number or house number.
vii. Passwords must be changed from time to time and even when suspected of being unknown to others.
viii. It made sense to change the default passwords provided by the software during installation

5. User login password must follow the same parameters described above.
6. Guest account should be disabled.
7. New devices with Windows 7 or 10 must run a built-in firewall.
8. All software on installed computer programs must be reinstalled from scratch (erase the hard drive and restart the installation disk).
9. Once the PC's hard disk is formatted, the OS and all software applications must be installed on the original software CDs. Only the data or document files should be copied from the old diskand care must be taken to ensure that no virus living on the old disk enters the newly formatted hard disk.
10. Generally, start in the most secure place (meaning no shares, no visitor access, etc.) and turn on the services if needed.

Guidelines to use Smart Boards

Smart boards have transformed the way teachers teach, including how they manage simple record-keeping tasks, engage student interest, illustrate complex concepts, assess learning, and prepare students for an evolving digital world. Like all other technologies, however, there are certain challenges for teachers trying to adopt smart boards. Here are a few guidelines that will help in maintaining interactive whiteboard:

1.To keep it interactive : Teachers report great success with having students come up and work out problems on the Smart Board in front of the classroom.

2. To utilize color: Teachers can make the text and background on the Smart Board any color they like, and they should take advantage of the brain's natural tendencies towards memorization.

3. Use the web: There are vast educational resources available online, from video to text to interactive applications. Whenever a teacher needs to flesh out a lesson, do a relevant search to find interesting resources.

4. Regular learning about the Smart Board : Teachers continue to discover new and innovative ways to use the Smart Board, and it requires just a short search online to find a plethora of ideas on how to use the tool.
5. Regular upkeep: Whiteboard is to be clean regularly using a dry eraser. Dry erasers for the said purpose can be taken from office supply store.
6. Thorough cleaning: Thorough cleaning can be performed using high-quality glass cleaner which helps remove any stubborn marks on the board.
7. Removing permanent marker ink: If a permanent marker has been used on the interactive whiteboard, use the dry erase marker to write over the permanent ink. Generally, the dry marker ink will help dissolve permanent ink marks.
8. Sensor cleaning: In case the pen sensors are not functioning, it may be caused due to accumulated dust. Use canned or pressurized air to remove the dust.

Smart board interactive whiteboard is a technological advancement that can be a great addition to a classroom or a workplace as they add value to meets and presentations. Use these tips to maintain the interactive whiteboard to keep it working efficiently for a long time.

POLICY ENFORCEMENT

- Violations of this policy by staff or faculty will be referred to the Principal and IT Cell of the College, respectively, for appropriate action and/or resolution.
- Violations of this policy by students or other non-College personnel will be referred to the IT Cell for appropriate action and/or resolution.
- Any use of the College's resources related to computer, by a student that constitutes plagiarism or cheating will be referred to the Judiciary Committee in accordance with the procedures as decided by management of the college.