ਸਨਾਤਨ ਧਰਮ ਕੰਨਿਆਂ ਮਹਾਂਵਿਦਿਆਲਾ ਮਾਨਸਾ–151505 (ਪੰਜਾਬ)

S.D. KANYA MAHAVIDYALA, MANSA-151505 (PB.)

(Affiliated to Punjabi University, Patiala)
An Education Crusading Women's Education Since 1970

Ref. No. SDKMV/__________ *Dated:________________*

IT Policy and Guidelines

Tables of Contents

Co-ordinator
IQAC
S.D. Kanya Mahavidyala, Mansa-151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

*Ref. No. SDKMV/*IQAC/IT/012/22

Dated: 11/8/22

Policy for Information and Technology

S. No	Policy Title: Policy for Information and Technology	Remarks
1	Administrative Policy Number (APN) SDKMV/IQAC/IT/012/22	**Functional Area:** Information and Technology Policy
2	Brief Description of the Policy	**Purpose:** To provide the latest information about the new developed technologies. **Audience:** All the faculty and students of the institution
3	Policy Applies to	All academic, administrative and managerial process in the organization.
4	Effective from the date	11 August, 2022
5	Approved by	SDKMV Mansa and Management Committee
6	Responsible Authority	IQAC Coordinator
7	Superseding Authority	Principal
8	Last Reviewed/Updated	New Policy
9	Reference for the policy	NAAC and NEP

Co-ordinator
IQAC
S.D. Kanya Mahavidyala, Mansa-151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

1. Need for IT policy

- IT policy is prepared and documented for fair and purpose to benefit students, faculty, Management and resources persons.
- Due to the policy initiative drives, IT resources utilization in the campus has grown by leaps and bounds during the last decade.

IT department of the college has been given the responsibility of running the institute's internet services. College is running the Firewall security, DHCP, DNS, email, web and applications restrictions and managing the network of the institute.

With the extensive use of the internet, network performance outreach in three ways:

- When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is potential bottleneck.
- When users are given free access to the internet, noncritical 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. Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service. Reducing Internet traffic is the answer.

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 downloads, file sharing and web surfing account themselves to files, replicate quickly and cause untold damage to information on the network.

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

Hence, in order to secure the network; IT cell 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 user 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.

Co-ordinator IQAC S.D. Kanya Mahavidyala, Mansa-151505

Principal, S.D. Kanya Mahavidyala, Mansa - 151505

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.

A college IT policy outlines guidelines for the use of technology and digital resources. It covers areas like acceptable use, network security, data privacy, software usage, and consequences for policy violations. The policy ensures a safe and productive technology environment for students and staff.

IT policies for colleges typically cover a range of areas, including:

- **Network and Internet Usage**: Guidelines on how students and faculty can use the college's network and internet resources, including acceptable use, prohibited activities, and bandwidth management.
- **Cyber security:** Policies related to data security, password management, access controls, encryption, and measures to protect sensitive information.
- **Software Usage**: Guidelines on software installation, licensing, updates, and restrictions on using unauthorized or pirated software.
- **Bring Your Own Device (BYOD):** Policies governing the use of personal devices on the college network, including security measures and restrictions.
- **Data Privacy:** Guidelines on how student and staff data is collected, stored, and used in compliance with data protection regulations.
- **Email and Communication:** Policies regarding email usage, communication etiquette, and rules for handling sensitive information through electronic means.
- **Social Media and Online Presence**: Guidelines for maintaining a professional and responsible online presence, especially for college-affiliated accounts.
- **Acceptable Use**: Clear guidelines on what is considered acceptable and unacceptable use of IT resources, including downloading copyrighted material, accessing inappropriate content, etc.
- **Remote Work and Learning**: Policies related to remote work and online learning, including security measures for accessing college resources from off-campus locations.
- **Incident Reporting**: Procedures for reporting IT security incidents, breaches, and potential vulnerabilities.
- **Backup and Data Recovery**: Policies for regular data backup, disaster recovery, and business continuity planning.

Co-ordinator IQAC S.D. Kanya Mahavidyala, Mansa-151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

- **Device and Equipment Usage**: Rules for proper usage, maintenance, and security of college-provided devices and equipment.

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 Centers, Laboratories, Offices of the institute 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 or off 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

2. Vision, Mission and Objectives

Vision:

To create a secure, innovative, and inclusive digital environment that empowers our organization to excel in the Digital Age.

Co-ordinator IQAC S.D. Kanya Mahavidyala, Mansa-151505

Principal, S.D. Kanya Mahavidyala, Mansa - 1515

Mission:

Our mission is to establish and uphold a comprehensive IT policy that safeguards data integrity, promotes responsible technology use, fosters continuous technological advancement, and ensures equitable access to digital resources for all stakeholders.

Objectives:

- **Security**: Implement robust cyber security measures to protect sensitive information and prevent unauthorized access.
- **Compliance**: Ensure compliance with relevant data protection and privacy regulations to maintain the trust of users and stakeholders.
- **Innovation:** Foster a culture of innovation by encouraging the exploration and adoption of emerging technologies that enhance productivity and efficiency.
- **Education:** Provide ongoing education and training to users to enhance their digital literacy and promote responsible technology use.
- **Resource Accessibility:** Ensure equitable access to digital resources, applications, and services for all members of the organization.
- **Continuity:** Develop a comprehensive business continuity and disaster recovery plan to minimize downtime in case of IT disruptions.
- **Collaboration:** Facilitate cross-functional collaboration to leverage technology for achieving organizational goals and objectives.

3. IT Hardware Installation Policy

The user community of the institute's network must observe certain precautions while installing their computers or peripherals so that he/she suffers the least possible inconvenience from the interruption of services due to hardware failure.

A. 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 earthling and have properly laid electrical wiring.

B. 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.

C. 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.

S.D. Kanya Mahavidyala Co-ordinator IQAC Mansa-151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

D. Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the institute centrally and distributed by the department, Institute Computer center will attend the complaints related to any maintenance related problems.

E. Non compliance

College Faculty, 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 effects 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.

4. Software Installation and licensing policy

Any computer purchases made by the individual Departments/projects 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 regarding respective 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.

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 IT Department.

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 CD/DVD other storage devices such as pen drives, external hard drives.

IQAC
Kanya Mahavidyala Mansa-151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

D. Noncompliance

Faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons.

An individual's non-compliant computer can have significant, adverse effects 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.

5.Network (Internet) Use Policy

Network connectivity provided through an authenticated network access connection or Wi-Fi is governed under the Institute IT Policy. The IT 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 IT Department.

A. Dial-up/Broadband Connections

Computer systems that are part of the Institute's campus-wide network, whether institute's property or personal property, should not be used for dial-up/broadband connections, as it violates the institute's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

B. Wireless Local Area Networks

This policy applies, in its entirety, to School, Department, or division wireless local area networks. In addition to the requirements of this policy, school, Departments, or divisions must register each wireless access point with computer center including Point of Contact information.

6. Email Account Use Policy

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 Institute communications are official notices from the Institute to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc..

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to **sdkmv mansa@yahoo.in** with their User **ID** and **password**. For obtaining the institute's email account, user may contact IT Department for email account and default password by applying in a prescribed format.

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

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of the institute's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to,

I.Q.A.C. Co-ordinator
S.D. Kanya Mahavidyala, Mansa 151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

- 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.
- 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.
- 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.
- 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.
- Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy.

7. Web Site Hosting Policy

A. Official Pages

The IT Center is responsible for maintaining the official web site of the institute viz., https:// sdkmvmansa.com only.

Beside keeping the web page updated all the information regarding of various departments.

B. Responsibilities for updating Web Pages

Departments, and individuals are responsible to send updated information time to time about their Web pages to IT Department.

8. Institute Database Use Policy

This Policy relates to the databases maintained by the institute.

Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential.

College 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 institute's approach to both the access and use of this institute resource.

- **Database Ownership:** S.D. Kanya Mahavidyala, Mansa is the data owner of entire Institute's institutional data generated in the institute.
- **Data Administrators:** Data administration activities outlined may be delegated to some of the officers in that Department.
- **MIS Components:** For the purpose of Management Information System requirements of the institute are:

S.D. Co-ordinator IQAC S.D. Kanya Mahavidyala Mansa-151505

Principal, S.D. Kanya Mahavidyala, Mansa - 151...

- Library Information Management System.

Here are some general policy guidelines and parameters for Sections, Departments and administrative unit data users:

a. The institute's data policies do not allow the distribution of data that is identifiable to a person outside the institute.

b. Data from the Institute's Database including data collected by Departments or individual faculty and staff, is for internal institute purposes only.

c. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the institute makes information and data available based on those responsibilities/rights.

d. 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 Office.

Such data tampering actions by institute member or outside members will result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

9. RESPONSIBILITIES OF IT DEPARTMENT

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by IT Department.
2. IT Department operates the campus network backbone such that service levels are maintained as required by the Institute Sections, Department s, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Maintenance of Computer Hardware & Peripherals

IT Department is responsible for maintenance of the institute owned computer systems and peripherals that are under warranty or out of the warranty.

C. Scope of Service

IT Department will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the institute and was loaded by the company as well as network related problems or services related to the network.

D. Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of IT Department.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of IT Department. It essentially means exactly at which location the fiberoptic based backbone terminates in the buildings will be decided by the IT Department. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of IT Department.

IQAC
Co-ordinator
S.D. Kanya Mahavidyala, Mansa-151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

3. IT Department will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
4. It is not the policy of the Institute to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the Institute's Internet links.

E. Network Expansion

Major network expansion is also the responsibility of IT Department. After every 3 to 5 years, IT Department reviews the existing networking facilities, and need for possible expansion.

F. Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations IT department considers providing network connection through wireless connectivity.
2. IT department is authorized to consider the applications of Sections, Departments, or divisions for the use of radio spectrum from IT department prior to implementation of wireless local area networks.
3. IT department is authorized to restrict network access to the Sections, Department s, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.

G. Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

H. Global Naming & IP Addressing

IT department is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. IT department monitors the network to ensure that such services are used properly.

I. Providing Net Access IDs and email Accounts

IT department provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the institute upon receiving the requests from the individuals on prescribed proforma.

K. Disconnect Authorization

IT Department will be constrained to disconnect any Section, Department, or division from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Section, Department, or division machine or network, IT department endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, Department, or division is disconnected, IT department provides the conditions that must be met to be reconnected.

Co-ordinator IQAC
S.D. Kanya Mahavidyala, Mansa-151505

Principal,
S.D. Kanya Mahavidyala,
Mansa - 151505

10.Video Surveillance Policy

The system comprises: Fixed position cameras, Monitors and 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 universities 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.

It is recognized that members of Institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the computer room.

Co-ordinator
IQAC
S.D. Kanya Mahavidyala, Mansa-151505

Principal
S.D. Kanya Mahavidyala,
Mansa - 151505