M.O.P. VAISHNAV COLLEGE FOR WOMEN (AUTONOMOUS)

(Affiliated to University of Madras, Re-accredited at 'A++' grade by NAAC)
Chennai – 600034

INFORMATION TECHNOLOGY POLICY

Rules and Regulations

Issuing Authority

IT Committee
Centre for Technical Support

M.O.P. Vaishnav College For Women (Autonomous)
(Affiliated to University of Madras, Re-accredited at 'A++' grade by NAAC)
20, IV Lane, Nungambakkam High Road,
Chennai – 600 034,
Tamil Nadu, India.

Signature of the Principal
Principal
M.O.P. Vaishnav College for Women
(Autonomous)
No. 20, IV Lane, Nungambakkam High Road
Chennai-600 034

M.O.P. VAISHNAV COLLEGE FOR WOMEN (AUTONOMOUS)
CHENNAI
600 034

Signature of the Committee Head

M.O.P. Vaishnav College for Women
(Autonomous)
No. 20, IV Lane, Nungambakkam High Road
Chennai-600 034

Contents

M.O.P. Vaishnav College for Women (Autonomous) provides access to high-end infrastructure and IT related services to students, researchers and teachers. The Centre for Technical Support maintains the policies governing the use of Information Technology services and resources at the College.

Need for IT Policy

The purpose of the IT policy is to maintain, secure, and ensure legal and appropriate use of Information Technology infrastructure established by the Institution. The policy aims to protect the confidentiality, integrity, and security of the information assets that are accessed, created, managed, and/or controlled by the College. The Information assets of the college include computer systems, network devices, software, intranet, internet services and other IT related services.

Objectives of IT policy

- To provide all required IT resources to all stakeholders as per academic guidelines laid down by UGC & AICTE.
- Leveraging IT as a tool for socio-economic development.
- Initiating and implementing green computing methods at the campus to create and foster an eco-friendly environment.
- To introduce new technologies to students on par with industry standards and evolving advancements.
- To ensure an effective annual maintenance plan which ensures maximum uptime of systems and devices.
- To ensure all IT resources are updated and available to students as per policies laid down by the college.
- To regularly monitor processes for software updates, firewall protection, anti-virus updating, network device status, system files cleaner, new web access policies, back-ups to ensure uptime of IT resources 24/7 to the stakeholders.

Roles & Responsibilities of the IT Committee

- Discuss, approve and implement IT related upgradation.
- Prepare the Annual IT Budget of the institution and place it for approval before the Principal and Management.
- Plan at the end of each academic year for the upgradation of IT infrastructure for the next academic year, to support evolving requirements of the learner and educator communities of the institution.
- Develop action plans to respond quickly and appropriately to IT maintenance issues and emergencies.
- Supervise all IT related work, and conduct annual stock taking of IT hardware and assets used for academic and admistrative purpose.
- Educate all teaching staff, non-teaching staff and students on the importance of sensitive and purposeful usage of computers and other IT related equipment on campus.
- Do regular checks of the computer stock registers maintained in the laboratories and learning centers.

Hardware and Software Procurement Policy

- All computer systems are purchased with warranty and after expiration of this warranty, they are efficiently maintained through an effective annual maintenance policy.
- Maintenance includes OS re-installation, virus scans, bandwidth capacity monitoring, internet downtime, communication cable fault, UPS monitoring, firewall renewal, antivirus upgrades, device replacements etc.
- All departments are provided with desktop computers with HD Cameras and Dolby Digital audio system, internet connectivity and a printer. These are for the use of department faculty members, who are responsible for ensuring compliance. Systems are purchased at the request of the Head of the Department. Troubleshooting / replacements are handled by external service engineers as per annual maintenance policy of the college.
- All systems and network devices are connected to electrical points through UPS. Regular 24/7 power supply is provided to webservers through recharging batteries. Regular battery maintenance is undertaken for all UPS.
- Care is taken at the time of installation to create separate paths for network cables distinct from those for electrical wires, to avoid noise in data communication.
- All files and printers shared through network are well protected with passwords to ensure integrity of data is maintained.

Hardware Installation Policy

- Computer systems on campus are administered by system administrators and system assistants
- All devices are installed by external service engineers.

Software Installation Policy & Licensing

- The Microsoft Campus Licensing agreement policy covers all computers on campus, and this license is renewed annually.
- OS is installed by external service engineers on call as per annual maintenance agreements.
- Application Software Licenses are maintained and renewed regularly to ensure valid and current updates to all application software.

Network (Intranet & Internet) Use Policy

The Technical Support Team is responsible for maintaining internet and intranet services of the college.

- The college has 212 Mbps internet bandwidth, with 112 Mbps from Airtel and 100 Mbps from ACT for running web server and application servers.
- All systems are networked.
- Firewalls are installed to provide protection against cyber-attacks or malicious network access attempts.

Wi-Fi Use Policy

- The Campus is fully Wi-fi enabled.
- Access points are located on all floors in the main block and the annex block, thereby giving access to all classrooms, seminar halls, laboratories, learning centres, staff rooms and the administrative wing.
- Each faculty is given an individual Wi-Fi ID and Password to access the internet.
- Students are also given Wi-Fi access.
- Access points are also added based on evolving requirements.
- Guests, resource persons and speakers are given access to Wi-Fi on request.
- Firewall protection and restricted access to certain websites are enabled to maximize security.

e-Mail Account Use Policy

- All faculty, students and administrative staff members are given individual institutional email ids (G-Suite) and password.
- Passwords are confidential and sharing such credentials is strictly prohibited.
- Attempting to access another member's login is strictly prohibited.
- All email communication must adhere to institutional and ethical guidelines, and should be completely free of offensive or controversial content (creation/distribution).
- Unlimited memory capacity is given to critical/important email ids.
- Users should not share their email account(s) with others.
- Students are given G-suite mail ID with unlimited space for online classes. They are also given access to all facilities offered by Google Workspace for Education.

Web Server & Cloud Hosting Policy

- The college maintains two webservers for its intranet and internet services.
- The college website is accessible at www.mopvc.edu.in. It is hosted on an external cloud platform. Information on the website is updated daily by an external maintenance agency.
- All intranet applications are run on the college-owned web servers.
- Users are given Login IDs and passwords to access server information, subject to restricted access policies.
- All systems networked to servers are given relevant IP addresses.
- Servers are protected from virus attacks and intrusions.
- Periodical updates of OS and other security software are systematically implemented.
- Regular backup processes are followed periodically.

Institute Database Usage Policy

- The institute has its own database creation and access to information policies.
- Information access is restricted for persons outside the institution.
- Any request for information/data is forwarded to the Principal's Office.
- Strict disciplinary action will be enforced in the unlikely event of any tampering or deletion of the institution's database.

Faculty Use Policy/Responsibilities of Departments

- Faculty members are responsible for computers and devices of their respective departments, and for ensuring compliance with institutional and process-specific policies.
- Passwords are confidential, and sharing these would be in direct violation of institutional policy.
- Use of institution resources for personal business gain, or for purposes which are inconsistent with the mission of the institution are prohibited.
- Unauthorized use of another's individual identification and authorization access is strictly prohibited.
- Using of institution networks HTTP, SSH, STP, EMAIL and private VPN etc. off-campus without prior approval is strictly prohibited.

Students Usage Policy/Responsibilities of Students

- Sharing of passwords, or other confidential information is strictly prohibited.
- Students are responsible for careful and judicious usage of computers in all Labs.
- Accessing another user's personal private data is not allowed.
- Downloading, sharing or using copyrighted material of institution including music, movies, software or textbooks without prior approval is prohibited.
- Connecting to the institution's restricted-access resources is prohibited.
- Connecting personal devices to the institution internet without approval is prohibited.
- Students must adhere to ethical guidelines, reflect academic honesty, and show restraint in the consumption of shared resources.

Video Surveillance Policy

- CCTV is installed in all classrooms, labs and on all floors.
- Videos are stored and archived on a regular basis.
- Unauthorized access to the Control Room is not permitted at any time.
- Footages are given on demand and with prior approval from the Principal.
- Cameras are serviced regularly.
- Live coverage is monitored by the Principal, Vice Principal and Administrative Head.

Anti-virus Protection and renewal Policy

- All computer systems in the college are covered under anti-virus protection.
- Application and Data Web Servers are secured with Kaspersky antivirus protection.
- Sophos firewall covers aspects of network security, email security, mobile security and unified threat management.
- Cisco Network Manageable switches provide a seamless network with secure, scalable and robust performance.
- Regular renewal and updating policies are in place for antivirus and firewalls and are implemented promptly.

Maintenance Policy for Systems and Network

- All Lab systems are maintained and overseen by lab assistants, system administrator and lab faculty in-charge.
- Technical problems such as power issues, booting, network problem, software installation, hardware troubleshooting, hardware replacement, and internet issues are handled by Lab assistants.
- Major Networking issues and Operating system failures are restored by System administrator and external service engineers on call.
- All Lab Computers are cleaned and serviced on regular basis.
- Regular system formats, junk clearance and cache clearance are performed at regular intervals.
- UPS maintenance and monitoring of battery levels are undertaken regularly.
- All Desktop systems are connected to network switches and maintenance of network cables are done regularly.
- Internet cables are well planned across the campus and networking is well designed.
- All systems and networking devices are covered under AMCs.

Online Classes and Online Examinations - Policy

- Google Workspace for Education is the official platform for all online classes.
- Faculty are enabled to create course classrooms and enroll students.
- All students are given individual login IDs and passwords to access G-classrooms
- Classes are scheduled through G-Meet, for which attendance is recorded by the respective faculty.
- Faculty regularly conduct assignments, quizzes and online assessments and evaluate the same through G-classrooms.
- End-semester examinations are also conducted using a separate Examination ID of the students and live proctoring will be done by the students.
- Valuators are given access to value answer script through G-classroom.
- Answer Scripts are downloaded and archived.

Guidelines for Students

- Access to institution resources engenders certain responsibilities and is subject to institution policies.
- Students must exhibit ethical usage behavior and reflect academic honesty at all times.
- Sharing of passwords and other authentic information is strictly prohibited.

Online Meetings/ Conferences/Workshops Policy

- Heads of Departments are given access control to create G-Meet meetings for Webinars/Conference/Workshops with prior approval from Principal.
- Departments are encouraged to use paid G-Suite or StreamYard integrated with YouTube to reach a larger audience.

Remote Support Policy

- The Technical Support team is responsible for enabling remote access.
- Remote access is given using tools such as Anydesk, Team Viewer to institutional members with prior permission from the Principal.

Backup and Restore Policy

- Application software and data are backed up periodically.
- Critical data are backed up daily and other application-specific data are backed up on a monthly basis.
- Lab servers, Web servers, Email Server, Website files and Cloud Server data backups are taken regularly and archived.
- Data is well preserved and protected against loss and destruction.
- Copies of backups are stored in a secured, off-site location.
- Backups are tested at regular intervals.