

St.Mira's College for Girls, Pune
(Autonomous, Affiliated to Savitribai Phule
Pune University)



[2017-2022]

IT Policy

St. Mira's College for Girls, Pune

Autonomous, Affiliated to Savitribai Phule Pune University

IT Policy

Purpose:

College maintains IT Policy to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established on the campus. This policy establishes the strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed by college.

While college is providing access to Internet to the faculty(teaching/non-teaching), students and staff with Limited Internet bandwidth, limited infrastructure like computers, computer laboratories to utilize.

This Policy applies to Students (UG and PG), Faculty(Teaching/Non-teaching) and Administrative Staff (Non-Technical / Technical).

IT Usage:

Following are the list of offences liable while using college IT infrastructure:

1. Tampering with computer source documents, records & developed software.
2. Hacking with a computer system.
3. Usage of the password, digital signature or other unique identification of another person.
4. Acts of cyber terrorism.
5. Publishing information which is obscene / defaming someone or any organization in electronic form.
6. Downloading of illegal software.
7. Attachment of any device that could bring viruses or damage to college computers.
8. Formatting of any computer in the college without permission.
9. Installation of software in college computers without permission.
10. Usage of computer peripherals (printers, scanners etc.) for personal work.



11. Photography of any material from the college computers, particularly during online exams, practicals & practical examinations.

To secure our college network , a firewall device is used that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between internal networks and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices.

For internal security, to protect our data from malicious attack we use antivirus 'Quickheal' for all devices and provide username and password for each user to access their data.



G. B. Gidwa

St. Mira's College for Girls