An Institution of
the Society for the Higher Education
of Women in India

Sophia College for Women
Empowered Autonomous

Bhulabhai Desai Road
Mumbai – 400026
Ph: 022-23512642 / 23523304

www.sophiacollegemumbai.com

ICT POLICY

1.	Administrative Policy Number (APN): SCWAPN/24	**Functional Area:** Refine institutional governance and communication with IT infrastructure and support.
2.	Brief Description of the Policy:	Purpose: Elevating IT infrastructure and security standards. Audience: All stakeholders of the organization.
3.	Policy Applies to:	All academic, administrative, and managerial processes in the organization
4.	Effective from the Date:	26th November ,2018
5.	Approved by:	College Development Committee (CDC)
6.	Responsible Authority	Lab Administrator
7.	Superseding Authority	Principal
8.	Last Reviewed/ Updated:	New policy
9.	Reason for the policy	Enhancing institutional governance through efficient IT infrastructure management and support.
10.	References for the policy	UGC/ NAAC/ University of Mumbai/ RUSA, etc

1. Introduction

As Sophia College for Women integrates technology more deeply into its educational framework, ensuring responsible and lawful use of Information Technology (IT) becomes essential. In line with the institution's commitment to offering industry-relevant programs, a robust IT policy is imperative to facilitate the safe and effective procurement, utilization, and maintenance of IT resources.

The college community, including faculty, staff, and students, relies extensively on a diverse range of information-technology resources. This Policy serves to complement existing standards and guidelines, delineating the specific rights and obligations pertaining to the use of the college's ICT facilities and electronic resources.

Following infrastructure resources are covered in ICT policy-

- Server
- Network Devices - Routers / Switches
- Computer Hardware
- Computer Software
- Security Cameras
- ICT Infrastructure Tools

2. Scope

This policy encompasses all Information Technology (IT) and electronic resources, referred to as "E-Resources," within Sophia College for Women. This includes but is not limited to computers, equipment, software, networks, and internet facilities owned or managed by the college, as well as any access or use of these resources from external systems. Additionally, it governs the handling of data, communication, and storage of information under the college's jurisdiction. Applicable to faculty, staff, students, alumni, and guests, this policy outlines the rights and responsibilities associated with accessing and utilizing the college's electronic resources.

3. Purpose

Sophia College for Women provides E-Resources to facilitate its academic and administrative objectives, prioritizing their use to advance these goals above all other purposes. While individuals within the college community may have diverse reasons for accessing and utilizing E-Resources, they share a collective responsibility to use them responsibly and safeguard them against unauthorized access or misuse.

4. Software and hardware purchase

Procurement of any new product is monitored by the Purchase Committee. The ICT purchase involves the following members.

- Management
- Principal and Vice Principals
- Network Administrator
- Website and Domain Administrator
- Staff members with IT Expertise

Steps for Purchase:

1. Staff or departments must submit detailed applications for their requirements.
2. Higher authorities review and approve the submitted requirements.
3. Multiple quotations are solicited from various vendors for the specified needs.
4. The purchasing committee evaluates the received quotations and may negotiate with vendors if necessary.
5. Upon finalization, a purchase order is issued to the selected vendor.

5. Hardware resources

- Server
- Networking Devices
- Desktop Computers
- Laptop Computers
- Printers / Scanners
- ICT tools
- Security Cameras
- Biometric Machine.

6. Software resources

- OS License
- Other Software Licenses
- Open-Source software products
- Antivirus Software.
- College Domain (for college website)

For the new purchase of any product above mentioned process is followed.

- The Head of Department and Subject Teacher will notify the lab administrator to download and install open-source software on designated computer systems as needed.
- For any updates to be made on the college website, staff must either send an email to the dedicated domain email address or submit a hardcopy application with authorized signatures to the domain administrator.
- To set up new employee or program email addresses, staff must either send an email to the dedicated domain email address or submit a hardcopy application with authorized signatures to the domain administrator.

7. Set-up

After successful delivery and basic installation from the vendor, the product is tested and stock entry should me marked in the register by office administrator.

8. Device Allocation :

- Following stock entry, products are labeled for the respective departments, and department heads or designated individuals will receive them. • Hardware devices are then installed within the departments.
- Training programs may be organized to familiarize faculty members with the usage of specific devices.
- Lab administrators are solely responsible for downloading and installing software packages. A schedule for installation is coordinated with relevant staff members or department heads to minimize disruption to office or laboratory operations.

9. Open-Source Software:

The lab administrator, with approval from the relevant Head of Department, will handle the downloading and installation of open-source software.

- Once installed, software is tested by the respective staff members for functionality. • Software licenses often require renewal based on the terms of the purchase agreement, typically every one or three years.
- Updates are applied similarly following the renewal process.
- A lab assistant is designated to maintain records of regular requirements and issues.

Internet Firewall is installed using a router.

- DHCP configuration
- Blocking of sensitive content
- Bandwidth control policy
- Antivirus

IP address is required for every system connected to the network. IP addresses are assigned for every laboratory, office, library.
Sensitive content and certain keywords are blocked for students. Social media websites and search engines can also be disabled for the time of examinations.

10. Software and hardware maintenance

- The Lab administrator oversees the systematic maintenance of IT infrastructure.
- Minor device repair or replacement tasks are managed by the lab administrator.
- Major device repair or replacement processes involve sending items off-campus with a gate pass entry to an external agency.
- Handling any uncommon hardware issues necessitates permission from the Head of Department and Principal.

11. Hardware maintenance

Before every semester's exam, all hardware equipment is inspected and cleaned. The lab administrator and assistants handle this task.

Every academic year, at the end, a routine stock update is taken. Peripheral device wear and tear is tracked.

To prevent any electrical problems like short circuits, all switches and electrical connections are regularly inspected.

Teaching staff members compile a list of any additional hardware device or component in accordance with the specifications of the syllabus for the following year.

12.Software maintenance

Every day, software fixes are released. When the internet connection is active, some of them are installed automatically. It is necessary to manually update the software packages if the automatic update option is not selected. Lab assistants carry out the task.

Regular upgrades are also necessary for open-source software.

The lab administrator will bring up the request with the principal if the license is renewable and when the renewal is due.

Software updates and new licenses can be received if the request is granted.

All client computers and the server, both, have up-to-date antivirus software installed.

Security Camera Maintenance / Recording

A company by name Advanced Emergency System Pvt Ltd is entrusted with maintaining the DVRs and security cameras under the monitoring of the of the institution

After receiving approval from the principal, anyone wishing to examine a recording for any reason—such as material loss or damage—must submit an application. From there, the recording can be scheduled for viewing.

13. Disposal

Reusable parts can be reused, and any that aren't will be given to the waste management facility.

14. Authorized Uses

E-Resources at Sophia College for Women are authorized for specific purposes aligned with the institution's mission and priorities, including work, study, research, and service activities. Academic and co-curricular uses are generally permissible if they adhere to college policies. Limited personal use supporting broader college objectives is also acknowledged, provided it remains incidental and does not result in additional costs to the college. It's important to recognize that utilizing E-Resources for personal purposes is a privilege, not a right, and should not disrupt their primary use for college-related activities.All use of E-Resources must comply with:

Users of E-Resources within Sophia College for Women must adhere to all institutional policies, procedures, and codes of conduct outlined in student, faculty, and employee handbooks. Additionally, they are required to comply with all relevant laws and regulations, as well as any applicable licenses and contractual agreements of the college, which may be updated periodicallyE-Resources may not be used, committed, or made available, without prior authorization, for:

- any ongoing business or other commercial activity not administered by the College;
- the benefit of persons or organizations other than the College; or
- political, communal or lobbying activities

The College has sole authority to determine what uses of E-Resources are proper and may prohibit or discipline use deemed inconsistent with this Policy or other applicable standards of conduct.

15. Email

Sophia College for Women may communicate official messages to its community members through electronic mail. It is the responsibility of students, faculty, and staff to regularly check their email accounts for college-related information. Employees are required to utilize their college email accounts exclusively for official college communications and refrain from using them for personal

16. Access Control:

User authentication via unique IDs and passwords is the primary means of accessing Sophia College for Women's E-Resources, ensuring protection against unauthorized entry and restricted data access. Users are strictly prohibited from sharing passwords and must promptly report any suspected compromise to the college's IT Staff. They bear full responsibility for activities conducted under their IDs and are reminded that no individual, including IT personnel, is authorized to request their password.

All users are required to safeguard the college's E-Resources from unauthorized access, adhering to the following guidelines:

Ensure the security and integrity of data stored on personal or assigned devices.
Access E-Resources only from secure environments and log out of sessions when leaving unattended computers.
Exercise caution when accessing confidential college data to prevent unauthorized disclosure or compromise.
Comply with directives from IT Staff and authorized personnel to discontinue activities that jeopardize the college or its resources.
Cooperate with system administrators during investigations of misuse.
Unauthorized actions include:

- Extending the network without authorization.
- Installing or altering software or hardware configurations without proper

authorization.

- Providing E-Resources or access to others.
- Sending unsolicited mass emails or altering email content or headers.
- Accessing data beyond authorized limits or attempting unauthorized data interception.
- Malicious use of the internet or network access.
- Tampering with system protections or introducing malicious code.
- Damaging computer or network systems.

Intellectual Property and Privacy:

Users must respect intellectual property rights, including copyrights, and comply with all applicable laws when using college E-Resources. Proper attribution is required for legally used copied material. Software usage must adhere to licensing agreements and legal provisions.

Users must also respect privacy rights, academic freedom, and freedom from harassment. Harassment or interference with others' use of E-Resources is prohibited. While the college generally respects user privacy, access to communications or data may occur under specific circumstances, such as maintaining system integrity or complying with legal obligations. Such access requires approval from competent college authority, except in emergencies necessary to preserve system integrity, comply with laws, or ensure health and safety.

A. P. Patil

IQAC Coordinator

Coordinator
IQAC
Sophia College

SOPHIA COLLEGE FOR WOMEN • MUMBAI 400026 •

Principal

PRINCIPAL, SOPHIA COLLEGE,
BHULABHAI DEASI ROAD,
MUMBAI-400 026.