SXCS/P-12

Information Technology (IT) Policy

SXCS is committed to helping all of its students reach their full potential. For this, the institution supports an extensive information-technology environment for faculty, staff, students, and other members of the community. There exists a Comprehensive Information and Technology Policy for all the SXCS Community members.

Scope

The IT usage applies to faculty, staff, students, and other members of the institution community who access or use the institution's e- resources (referred to in this policy as 'users') including without limitation, the faculty, staff, students, alumni, and guests.

For all pertinent activities involving the institution's students, this policy applies to campus activities, placement-organizations subject to the implementing legal and mandatory regulations of UGC. This policy applies to all information-technology and other electronic resources (e-resources) of the institution, including without limitation:

- All computers, systems, equipment, software, networks, and computer facilities owned, managed, or maintained by the Institution for the handling of data, voice, television, telephone, or related signals or information.
- Any access or use of the Institution's electronic resources from a computer or other system not controlled or maintained by the Institution; and,
- The creation, processing, communication, distribution, storage, and disposal of information under the Institution's control.

In addition, members of the institution may have access to third-

party electronic resources through their affiliation with the institution, including the resources of other sister institution/institution (St. Joseph's Institution of Management or of any other contracting party of the Institution). Use of these resources by members of the institution is governed by this policy and any applicable policy or restriction of the third-party provider.

Policy Summary

This policy applies to campus activities, contracted organizations, and student activities. The policy also explains the roles of those working with maintaining, operating, and overseeing institution e- resources. The staff of the institution (IT staff) are responsible for the administration of this policy.

Introduction

Information technology is an important resource in today's world. The institution and all its staff members are legally obligated to protect the sensitive data of the institution. The computer resources of SXCS are available to authorized students, faculty, administrators, and staff for educational, research, and administrative purposes.

Purpose

The institution makes IT resources available to support its academic and administrative goals. Within the institution, different users will have varying purposes of using and accessing IT- based resources and will have a shared responsibility to utilize the resources appropriately and protect them from unauthorized access or usage. Institution Information Resources and Institution Data is used, managed, and protected appropriately to ensure that they are:

Available

Accurate and complete, and

Disclosed appropriately when required.

Definitions

The term IT-Resources includes Email, Accounts and Access, E-Resources (remote or otherwise), College MIS data available on the intranet and internet, and physical resources such as servers, laptops, firewalls, antivirus, network switches, access points.

Email

The Institution may send official correspondence to members of its community via electronic mail. Students, faculty and staff are expected to check their @sxcsim.ac.in email accounts regularly and are responsible for the information sent there. Institution's employees are expected to use their SXCS, official email accounts for all Institution-related communications.

If a student elects to forward his/her @sxcsim.ac.in email to another email account, the student remains responsible for any material not received because of any defect in the forwarding mechanism or the destination account.

Accounts and Access Restrictions

- The primary methods used to authenticate users of the College's e- resources are User IDs and passwords. Unauthorized access to e- resources or any restricted information found within them are prevented by this primary method.
- It is expected that all users will not share their passwords with any other person and would protect them from disclosure especially with student community, keep changing them regularly, and also monitor access to their accounts.
- They are expected to contact IT staff if they suspect their passwords or user-ids have been compromised.

E- Resources

E-resources may be used only for the purposes authorized by the College. These purposes generally comprise work, study, research,

service, or student residential activities consistent with the College's mission and priorities.

Use of e-resources in connection with activities such as learned societies, professional associations, academic conferences, the preparation of scholarly publications, and other educational institutions' tenure or departmental reviews, occasionally with incidental compensation is generally acceptable as long as the activities are otherwise consistent with the Institution's mission and policies.

All use of e-resources must comply with:

- Institution policies, procedures, and codes of conduct, including those found in the student, faculty, and employee handbooks.
- All laws and regulations applicable to the user or the Institution; and,
- The Institution 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.

Prohibited under the usage of IT Resources

- Requisition of any user's password by any person including any member of the IT staff other than the owner, is not permitted under any circumstances.
- Use the College's Internet or other network access in a malicious manner or to alter or destroy any material which the user is not authorized to alter or destroy;
- Tamper with, modify, damage, alter, or attempt to defeat restrictions or protection placed on accounts or any e-resources; or
- Damage computer or network systems; create or intentionally introduce or propagate computer viruses, worms, or other malicious code to any e-resource; attempt to degrade the performance of the system or to deprive authorized users of e-resources or access toe-resources.

Usage Policy

It is expected that all staff members will use the IT- resources for the purpose in which they are intended to, in a responsible, ethical, and lawful manner. While performing their duties, SXCS staff members have access to a wide range of confidential information about students, staff and the Institution in general. Information is expected to be accessed only for the purpose of fulfilling job duties. Such information accessed would not be shared or used either internally or externally for any purpose other than its intended use.

Hardware and software available at the campus are maintained by constant monitoring of usage, protection from virus, preventives of abuse of software, suitable policies to block use social websites is implemented in the firewall. All equipments are protected with UPS to avoid loss of data in case of power failure.

ICT Infrastructure

SN	Descriptions	Location
1.	Desktop Computers	Computer Labl
		Computer Lab2
		Library
		Staff
		Admin Office
2.	Internet	Campus
3.	Server	Campus
	Firewall	Server Room in campus
4. Projectors		Classrooms
		Others (Board Room, Audi, Conference AV Room)
5. CCTV Cameras		Campus
6. Laptops		Lab & Staff
7. Biometric Systems		Office
8. Digital signage TV		Campus
10. Printing & Scanning		Campus

Operational Procedures

- All users are having individual login id & password to access ERP, Email etc.,
- Laptops are issued to staff for their official usage inside the college.
- Students produce their ID Card when demanded by the Institution Staff inside the Computer Lab
- The students are given unique credentials to access the computers and laptop available in the Institution premises.
- The data accessed by students are maintained with proper data Security policy and protocol in the server.
- The faculty members are provided with official email ids for communicating with stakeholders (internal/external).
- Data related to the accounts section, the examination section and the library are kept in backup files on a regular basis.
- In order to ensure data security, virus issues, access to pen drives is not made available
- Use of Mobile Phones, games and music are strictly prohibited in the Computer Lab
- Eatables & Soft Drinks of any kind are strictly forbidden inside the Computer Lab