St. Xavier’s College (Autonomous), Mumbai

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY

Policy Measures

- Information technology resources are central to the educational mission of St. Xavier's College. Students, faculty, and staff must respect the rights of others, abide by all college policies and applicable state and UGC rules, and assume shared responsibility for safeguarding the college's information technology environment
- St. Xavier's College's computing resources may not be used for any activity that is illegal, unethical, or contrary to the educational goals of the college. Freedom of expression and the existence of an open environment conducive to inquiry and learning will be respected by the college with regard to use of information technology resources, but behaviour that constitutes misconduct will not be protected.
- To enable the appropriate educational and administrative use of information technology resources, the college provides a secure network. Without connectivity standards, our campus community is at risk to damage from hardware or software that has not been appropriately configured or maintained. These damages could include financial losses, interruption of network services, and the loss of data. To minimize exposure to such damages, this policy also defines standards for connecting computers, servers, or other devices to the college’s network.

SCOPE

All financial and administrative policies involving community members across campus are within the scope of this policy. If there is variance between departmental expectations and the common approach described through college policy, the college will look to the campus community to support the spirit and the objectives of college policy.

Authorities Delegated and Retained/Administrative Responsibility

The Principal of the college delegates administration of the college’s Acceptable Use Policy to the chief technology officer/Director for information technology.

General Use

Common sense and respect for others are excellent guides to what constitutes appropriate behaviour in the use of information technology resources. Prohibited conduct falls into several areas including but not limited to unauthorized access, copyright violations, acts of destruction, invasion of privacy, and harassment. The policies listed below are not exhaustive but should convey a broad sense of what behaviour constitutes illegal, unethical, or inappropriate conduct. As in other aspects of college life, users are bound by the policies and guidelines published on the St. Xavier's College (SXC) policies website and in St. Xavier's College Handbooks. By using SXC information technology resources, students, faculty, staff, and others agree that they are familiar with and will abide by those policies as well as this acceptable use policy and any modifications made thereto in the future.

ACCOUNT/SYSTEM ACCESS

Unauthorized Account or System Use

Users may not access data or other information technology resources without proper authorization, regardless of whether any damage is done or whether the data or other information technology resource in question is owned by the college.

1. Users may not access or use, or attempt to access or use, any network accounts other than their own assigned accounts or any system for which they have not been granted access. In other words, users should use only their own files, those that have been designated as public, or those that have been made available to them with the knowledge and consent of the owner.
2. The college's Honor Code and its prohibitions against plagiarism and cheating, among other things, applies to student use of any files and information obtained from SXC's information technology resources when used in the preparation of academic coursework.
3. Passwords should not be revealed to anyone else and should be changed according to published password standards.
4. Users may not attempt to determine the password of another person through any means.
5. Impersonation of another person by sending forged information (e.g., sending email with an erroneous "sender") is prohibited.

Appropriate Connection Methods

Devices may only be connected to the college's network at appropriate connectivity points via authorized methods.

1. Users may not make modifications or extensions to the network, such as installing a personal wireless access point that rebroadcasts the College's network.
2. Users should consult XKC if they discover a need to modify or extend the network.

Network Registration

Those using the college's network may be required to authenticate when connecting a device. XKC maintains a database containing machine identification, network addresses, and ownership information. This data is used to contact the registered users of the equipment in the event their devices are compromised.

Protection of the Network

XKC uses multiple methods to protect the college's network. These include monitoring for external attacks, scanning the network for anomalies, and proactively blocking harmful traffic. There may be times where more extensive procedures are required to address potential security exposures or to contain actual security exposures.

1. SXC uses SOPHOS UTM to ensure the following:
    a. **Web Protection** Comprehensive protection from the latest web threats and powerful policy tools ensures users are secure and productive online.
    b. **Email Protection** Full SMTP and POP message protection from spam, phishing and data loss with our unique all-in-one protection that combines policy-based email encryption with DLP and anti-spam.
    c. **Network Protection** to stop sophisticated attacks and advanced threats while providing secure network access
2. By connecting to the college's network, users acknowledge that network traffic to and from their devices may be scanned.
3. By connecting to the college's network, users acknowledge that if a device exhibits behaviour that XKC believes to be a risk, the device will be removed from the network.
4. Suspicious device behaviours include:
    a. Using substantial network resources,
    b. Sending disruptive network traffic, or
    c. Exhibiting a pattern associated with scans or attacks.

Suspension or Revocation of Access

Use of SXC information technology resources is a privilege. If a person is found to be in violation of these policies, this privilege may be revoked through temporary or permanent denial of access to such resources.

People suspected of violating these policies may be temporarily denied access to SXC's information technology resources during investigation of the alleged abuse.

Additional Consequences of Misuse

Abusers of the college's information technology resources will be subject to existing disciplinary procedures under current college policies in accordance with the abuser's campus status. When appropriate or required by law, the college may request or provide assistance to law enforcement agencies to investigate suspected illegal activities.

Harassment

Information technology resources may not be used to intimidate, threaten, or harass other individuals.

St. Xavier's College's information technology resources may not be used for any activities that violate the college's Anti-Discrimination Policy, Student Code of Conduct, workplace standards, or state or UGC laws.

Information technology resources may not be intentionally used to view, store, print, or send obscene materials or slanderous, harassing, or threatening messages.

Confidentiality

St. Xavier's College has both an ethical and legal responsibility to protect the confidential information of users. Confidential data is defined by local, state, and UGC law. To promote confidentiality users must not:

1. Perpetrate, cause, or in any way enable security breaches, including but not limited to accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access;

2. Facilitate use or access by unauthorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends;

3. Share private, financial, or personally identifiable information (i.e., SSN, tax information, student IDs, etc., according to state law), even in the case when users are accidentally granted permissions to files or folders they should not access by means not approved for transmission of college information;

4. Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password.

Copyright and License Protections

1. The author of a text or the creator of a graphic, program, or application is protected by copyright law unless they specifically release that work into the public domain. In accordance with the college's policies governing the treatment of copyrighted materials, users should always obtain written permission from the original author(s) before copying electronic materials that are not in the public domain.
2. No user may copy or attempt to copy any proprietary or licensed software provided by or installed on college-owned resources. Copyright laws and license agreements protect much of the software and data that reside on the college's systems.
3. Unauthorized duplication of software may subject users and the college to both civil and criminal penalties under the IT Copyright Act.
4. Stolen or bootleg copies of software are not allowed on any College computing systems.
5. All software programs must be registered in accordance with their license and use provisions.

Privacy

The campus network is maintained and provided to assist in the pursuit of the mission of St. Xavier's College and to conduct the College's day-to-day operational activities. The network is College property thus all data composed and created by employees and transmitted and/or stored on the network, is and will remain College property, not the private property of any individual.

St. Xavier's College will make every reasonable effort to respect a user's privacy.

1. Users should have no expectation of privacy for communications, documents, or other data transmitted or stored on the organization's resources. In addition, in response to a judicial order or any other action required by law or permitted by official College policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the organization, the College reserves the right to access, review, intercept, monitor, and/or disclose all data created, transmitted, accessed, and/or stored on the College's network and/or technology.
2. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the organization's rules, regulations, or policy, or when access is considered necessary to conduct College business due to the unexpected absence of an employee or to respond to health or safety emergencies.
3. Any personal or college-owned data created, transmitted, accessed, and/or stored on the campus network by users on personally owned devices is subject to the same policies, procedures, guidelines and constraints as data created, transmitted, accessed, and/or stored through the use of College-owned devices.

4. Exceptions to the data ownership clause described includes: student works developed as a part of their academic or co-curricular pursuits; and scholarly work by faculty and staff such as articles, books, music composition, research data, and the like.

Violation of Privacy

1. Information, data files, external devices, email, and programs owned by individual people are considered private, whether or not the information is accessible by others.
2. Access to private, financial, or personally identifiable information is restricted to authorized users, even in the case when users are accidentally granted permissions to files or folders they should not see.
3. Tampering with email, interfering with or intercepting its delivery, and using email for criminal purposes may be a felony offence. The Information Technology Act 2000 places electronic mail in the same category as messages delivered by the Postal Service.