IT & Internet Usage Policy

1. Overview

Internet connectivity presents with new dangers that must be routed to safeguard the facilities, vital information assets. Access to the internet is provided to faculties, staff and students (additionally alluded as users) to help scholarly exercises.

The College’s specialized assets – including desktop and portable computer systems, fax machines, Internet and World Wide Web get to, voice message, electronic mail (email), SMS Service, electronic announcement sheets, and its intranet – are clearly an essential and vital piece of its business. Since these advances are both new and quickly transforming, it is essential to clarify how they fit inside the College and inside your obligations.

2. Purpose and Scope of the document

- The reason for this policy is to characterize the proper utilization of the of the internet by the students, faculties and staff of the Shah and Anchor Kutchhi Engineering College (SAKEC).
- This policy applies to all internet users (Faculty, Technical staff, Administrative staff, Contract/Temporary staff and Students (BE/ME) who access the internet facility provided by the SAKEC through Wired or WiFi networking. The internet users are relied upon to be comfortable with and to consent to this policy.

3. Internet Access Usage

- Users not conforming to these policies could be liable to disciplinary action. Internet access will be discontinued upon completion of a study of student, completion of the contract, transfer of faculty/staff, or any disciplinary action arising from violation of this policy.
- The privileges granted to users and are being rigorously monitored and may be revoked at any time if it is no longer needed by the user.
- Internet users of SAKEC shall comply with applicable National/State/Cyber laws and rules and policies of SAKEC. Examples of Rules and policies include the laws of privacy, copyright, trademark, obscenity and pornography. The IT act 2000 which prohibit hacking, cracking, spoofing and similar activities.
- According to the SAKEC IT policy, the tethering/hotspotting of internet connection is liable for deactivating the connection. Users will be required to obtain necessary authorisation before using college connectivity.
4. **Usage Policy of xyz@sakee.ac.in Account:**

- Users will also be responsible or any activity originating from their account. In case of unauthorized use of the account, detected or suspected, the account owner should change the password and report the incident to Principal immediately.
- Users shall not use college network and connectivity to get unauthorised access to remote computers.
- The College asks you to keep in mind that when you are using the College’s computer you are creating College documents using a College asset. The College respects the individual privacy of its staff. However, that privacy does not extend to a staffs conduct or to the use of College-provided technical resources or supplies.
- The College’s computer, voicemail, e-mail, or telephone systems, and the data stored on them are and remain at all times the property of the College. As a result, computer data, voicemail messages, e-mail messages, and other data are readily available to numerous persons. If during the course of your employment, you perform or transmit work on the College’s computer system and other technical resources, your work may be subject to the investigation, search, and review of others in accordance with this policy.
- All information, including e-mail messages and files, that are created, sent, or retrieved over the College’s technical resources is the property of the College, and should not be considered private or confidential. Staff have no right to privacy as to any information or file transmitted or stored through the College’s computer, voicemail, e-mail, or telephone systems. Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate educational interests and obligations of the College. Staff should also be aware that, even when a file or message is erased or a visit to an Internet or Web site is closed, it is still possible to recreate the message or locate the Web site.
- The College reserves the right to monitor your use of its technical resources at any time. All information including text and images may be disclosed to law enforcement or to other third parties without prior consent of the sender or the receiver.

5. **Prohibited Downloads**

The following downloads are specifically not allowed on computers unless approved. Theft or other abuse of the campus network, computers, or computer time, including but not limited to:

- Unauthorized entry into a file to use, read, or change the contents or for any other purpose.
- Unauthorized transfer of a file.
- Unauthorized use of another individual’s identification or password.
• Use of computers or computing facilities and resources to interfere with the work of another student, faculty member, or University official.
• Use of computing facilities and resources in violation of copyright laws.
• Illegal Use: Transmission, distribution, or storage of any material in violation of an applicable law or regulation is prohibited. This includes, without limitation, pornography, viruses, worms, or harmful code, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization.
• Threats: Threats of bodily harm or destruction of property, or any other communication that constitutes an illegal threat or harassment.
• Reselling: The resale of Internet Service or otherwise making available to anyone outside the premises the ability to use the Service (i.e. Wi-Fi, or other methods of networking) without proper authorization.
• Impersonation/Forgery: The use of the Internet Service for the impersonation of another person for any purpose, including, without limitation, adding, removing, or modifying email or network header information, use of free email services, selling or auction services, and chat or other instant messaging services.
• Email: Sending unsolicited mail messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (“email spam”). This includes, without limitation, bulk-mailing of commercial advertising, informational announcements, and political tracts.
• Use of any technology to create, display or distribute an audio, video, digital file, picture or film of another individual without that person’s knowledge and consent while the person is in a place the individual would have a reasonable expectation of privacy.
• Any peer to peer file sharing application: Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer. So users should thus refrain from such activities.
• Any third party personal antivirus or firewall: Since adequate security has already been provided for all machines via pre-defined firewall rules, third-party firewalls may interfere with these rules thus endangering the network.
• Any Proxy servers, private firewall, tunnelling software, connectivity sharing software
• Hacking tools of any sort: The use of any such tools on a college network is strictly prohibited. Games & Movie trailers or previews.
• Any other copyrighted content/materials/software which is not appropriate to the user or institute
6. **Enforcement**

- Users found violating this policy may be subject to penalties and disciplinary action.
- The SAKEC network admin may suspend, block or restrict the access to an account when it reasonably appears necessary to do so in order to protect the security, integrity or functionality of the network.
- Suspected violations of applicable laws may be referred to appropriate law enforcement agencies.

7. **Your Responsibilities**

Each user is responsible for the content of all text, audio, or images that they place or send over the College’s technical resources. Staff may access only files or programs, whether computerized or not, that they have permission to enter.

Violations of any guidelines in this policy may result in disciplinary action up to and including expulsion. In addition, the College may advise appropriate legal officials of any illegal violations and cooperate in investigations conducted by legal officials.

Use of the Internet (wired or wireless) is not intended for the following:

- Operation of a business or other commercial use
- Solicitation for personal gain
- Sending chain letters or spamming
- Gambling
- Downloading Movies and games.
- Viewing movies and playing games
- Accessing stockbroking sites and dealings with Stock Market
- Malicious actions, such as denial of service attacks
- Harassment of other computer users
- Accessing and/or distribution of pornographic materials
- Copyright violations
- The offering of network or Internet access services
- Bit-torrents, File-sharing or other bandwidth-intensive applications that may degrade the quality of service
- Wireless spectrum interference or disruption of other authorized communications
- Engaging in any other activity in violation of local or state or central law
The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. To ensure a virus-free environment, only the Network Admin is authorized to download/install files and software from the Internet onto college-owned devices.

8. **Disclaimer**

- SAKEC reserves the right to send messages (SMS) to all Users (staff & Students) using SAKEC SMS system.
- SAKEC reserves the right, without notice, to limit or restrict individual’s use and to inspect, copy, remove or otherwise alter any data, file or system which may undermine the authorized use of any computing facility or which is used in violation of SAKEC rules and policies.
- SAKEC also reserves the right periodically to examine any system and other usage and account activity history as necessary to protect its computing facilities.
- SAKEC disclaims any responsibility for loss of data or inference with files resulting from its effort to maintain security and privacy.
- SAKEC reserves the right to amend these policies at any time without prior notice and to take necessary action to comply with applicable laws.