Internet Usage and Security Policy

MARIAN COLLEGE KUTTIKKANAM (AUTONOMOUS)
MAKING COMPLETE

1. Overview

Internet connectivity presents with new risks that must be addressed to safeguard the facilities and vital information assets. Access to the Internet by users that is inconsistent with academic needs is deemed to be misuse of resources.

2. Purpose and Scope of the document

The purpose of this policy is to define the appropriate use of internet by students, faculty and staff of Marian College, Kuttikkanam.

This policy applies to all internet users (Faculty, technical staff, administrative staff, contract/temporary staff, students and research scholars) who access the internet facility provided by the Marian Computer Lab (MCL) through Wired or Wi Fi networking. The internet users are expected to be familiar with and to comply with this p o l i c y .

3. Internet Access Request and Approval

Internet access will be provided to users for their academic needs only and they are restricted to access the contents under the academic category o n l y .

As part of the Internet access request process, the user is required to read the Internet usage and Security Policy. The user must sign the declaration in the application that they understand and agrees to comply with the policy guidelines. Users not complying with these policies are liable to be subjected to disciplinary action.

3.1. Application Procedure

- Students: All the students are required to submit an internet access request form to the MCL.
- Faculty/Staff: Faculty and staff members have to submit their duly signed request to the lab for getting the access.

3.2 Removal of Access

Internet access will be discontinued upon completion of study of student, completion of contract, transfer of faculty/staff or if any disciplinary action arising from violation of this policy arises.

The privileges granted to users may be monitored and may be revoked at any time if it is no longer required to be provided to the user.

4. Usage Policy

4.1. General Guidelines

- Internet users of Marian College shall comply with applicable National/State/Cyber laws and rules and policies of Marian Sophos Firewall. Examples of rules and policies include, the laws of privacy, copy right, trade mark, obscenity and pornography, and the Information Technology Act, 2000 which prohibits hacking, cracking, spoofing and similar activities.
- According to the Marian policy, the tethering/hot spotting of internet connection is liable for deactivating the connection.
- Users will be required to obtain necessary authorization before using college connectivity.
- Users will also be responsible for any activity originating from their account

4.2. Security and Privacy

- Users should engage in safe computing practices by establishing appropriate access restrictions for their account and computing devices, guarding their password and changing them regularly.
- The College, in its discretion may disclose the results of any such general or individual monitoring including the contents and records of communication to the appropriate authorities or law enforcement agencies and may use those results for disciplinary procedures.

4.3. Prohibited Downloads

- 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.
- Any third-party personal antivirus or firewall: Since adequate security has already been provided for on all machines via pre-defined firewall rules, third party firewalls may interfere with these rules thus endangering the n e t w o r k .
- Any Proxy servers, private fire wall, tunnelling software, connectivity sharing software
- Hacking tools of any sort: The use of any such tools on college network is strictly prohibited.
- Auction sites
- Dating sites
- Gambling sites
- Game sites
- Any other copyrighted content/materials/software which are not appropriate to the user

4.4. Wi-Fi Policy

- College Wi-Fi is available in the whole campus and hostels.
- The access to college Wi-Fi is restricted to registered users who want to avail the Wi-Fi facility.
- The access to college Wi-Fi is restricted to the registered device only. Usage of college Wi-Fi in an unregistered device by spoofing/tethering will be treated as violation of this policy.
- Even if the access id is different, the registered Wi-Fi user is the sole responsible person for all communications originating from the registered device.

4.5. Enforcement

- Users found violating this policy may be denied access to the Marian network for a minimum period of six months and may be subject to other penalties and disciplinary action.
- Suspected violations of applicable laws may be referred to appropriate law enforcement agencies.
- Alleged violations will be handled through MCL disciplinary procedures applicable to the user.

5. Disclaimer

- Marian Networks 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 Marian college rules and policies.
- Marian Networks also reserves the right periodically to examine any system and other usage and account activity history as necessary to protect its computing facilities.
- Marian Networks disclaims any responsibility for loss of data or inference with files resulting from its effort to maintain security and p r i v a c y .
- Marian Networks reserves the right to amend these policies at any time without prior notice and to take necessary action to comply with applicable l a w s .

Internet Usage and Security Policy

MARIAN COLLEGE KUTTIKKANAM (AUTONOMOUS)
MAKING COMPLETE

General Do's	General Don'ts
1. Do respect the rule "That which is not expressively permitted is prohibited".	1. Do not download content from Internet sites unless it is related to your work.
2. Do use the internet only for academic related matters	2. Do not make any unauthorized entry into any computer or network.
3. Do check the information you access is accurate, complete and current.	3. Do not represent yourself as another person. Do not share your password.
4. Do respect the legal protections to data and software provided by copyright and licenses.	4. Do not use Internet services to transmit confidential, political, threatening, obscene or harassing materials.
5. Do inform the Marian lab in case of any unusual occurrence.	5. Do not attach/transmit files through email which contains illegal/unauthorized materials.
6. Do contact the Marian lab in case of any Internet related problems.	6. Do not use Marian network for Peer-to-peer file sharing.
7. Do clean the browser history and cache periodically.	7. Do not download any image/video/file which contain pornographic, racist, violence or any illegal activity.
8. Do sign off from captive portal when you are not using Internet or leaving the system.	8. Do not use Internet services to download movies/previews/Games.

Monitoring and Enforcement

a. Sophos firewall XGS 5500 shall track the usage, or examine the content,