1. Overview

The usage of information technology transformed all the activities in the world tremendously more so the academic activities of the institutions. Many activities in the institutes are done online, computers, laptops, and smartphones and hence ensuring the best internet security is the way forward to keep our identities, documents, and passwords are not compromised. With a majority of Internet connectivity presents new risks that must be addressed to safeguard the facilities, and vital information assets. Access to the internet will be provided to faculty, staff, and students (further referred as users) to support academic activities. Access to the Internet by users that is inconsistent with academic needs results in the misuse of resources.

2. Purpose and Scope of the document

The purpose of this policy is to define the appropriate uses of the Internet by the students, faculty and staff of MDC.

This policy applies to all Internet users who access the Internet facility provided by MDC through Wired or WiFi medium. The Internet users are expected to be familiar with and to comply with this policy.

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 for academic purposes only.

-2-

As a 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 agree to comply with the policies. Users not complying with these policies could be subjected to disciplinary action.

Application Procedure

- *Students:* All the students are required to submit the Internet access request form to the MDCIT Deptt. through the HOD.
- *Faculty/Staff:* Faculty and staff members have to submit their duly signed request to the MDCIT Deptt. through the HoD to get access.

Approval and Access

Applications will be examined and approved by MDCIT Deptt. All the activities using this user id is logged at the MDCIT Deptt. and the user is solemnly responsible for the activities associated with their user id.

Removal of Access

Internet access will be discontinued upon completion of the study of student, faculty/staff leaving the institute permanently, or any disciplinary action arising from violation of this policy.

The privileges granted to users are continuously monitored and may be revoked at any time if it is no longer needed by the user.

4. Usage Policy

General Guidelines

➢ Internet users of MDC shall comply with applicable National/State/Cyber laws and rules and policies of MDC. Examples of rules and policies include, the laws of privacy, copy right, trade mark, obscenity and pornography. The IT act of government prohibits hacking, cracking, spoofing and similar activities.

➢ According to the MDC policy, tethering/hot spotting of internet connection is liable for deactivating the connection.

➢ Users will be required to obtain necessary authorization before using institute connectivity.

➢ Users will also be responsible for any activity originating from their account.

➢ Accounts and passwords should not under any circumstances be used by any other persons other than those to whom they have been assigned by website committee of MDCIT

➢ In case of unauthorized use of account is detected or suspected, the account owner should change the password and report the incident to website committee of MDCIT.

➢ Users shall not use institute network and connectivity to get unauthorized access to remote computers which may damage the operations of MDCIT Network.

-4-

Security and Privacy

- Users should engage safe computing practices by establishing appropriate access restrictions for their account and computing devices, guarding their password and changing them regularly.

- Users should note that their use of institute connectivity is not completely private. As a part of security measure, all the activities are logged and monitored at MDCIT Deptt.

- The institute, 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.

Prohibited Downloads

The following downloads are specifically not allowed on computers unless approved in writing by MDCIT Deptt.

- 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 all machines via pre-defined firewall rules, third-party firewalls may interfere with these rules thus endangering the network.

➤ Any Proxy servers, private fire wall, tunnelling software, connectivity sharing software

➤ Hacking tools of any sort: The use of any such tools on institute network is strictly prohibited.

➤ Games & Movies

➤ Any other copyrighted content/materials/software which are not appropriate to the user

WiFi Policy

➤ Institute WiFi is available in the whole campus and hostels. WiFi will not be available at hostels during class hours.

➤ The access to institute WiFi is restricted to registered users. The one who wants to avail the WiFi facility, has to submit an application in the prescribed format and personally bring the device to register at MDC IT Policy.

➤ The access to institute WiFi is restricted to the registered device only. Usage of institute WiFi in an unregistered device by spoofing/tethering will be treated as violation of this policy.

➤ Even if the access id is different, the registered WiFi user is the sole responsible person for all the communications originated from the registered device.

Enforcement

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

Disclaimer

- MDC IT 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 MDC IT rules and policies.
- MDC IT also reserves the right to periodically examine any system usage and account activity history as necessary to protect its computing facilities.
- MDC IT disclaims any responsibility for loss of data or inference with files, resulting from its effort to maintain security and privacy.

MANSAROVAR DENTAL COLLEGE
INFORMATION TECHNOLOGY (IT) Policy

5. Do's & Don'ts

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

❀❀❀❀❀❀