

Indian Institute of Technology Indore IT Usage Policy (Ver.1.0)

IT infrastructure refers to an enterprise's entire collection of hardware (computer, laptop, tablet or mobile device, web server), software, networks (NKN internet or Wi-Fi), web and mobile applications, printing and scanning devices, electronic screens, projectors, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services.

In its endeavor to provide all faculty, students and staff with a modern, fully networked computing and IT environment for official use, the IT Policy is implemented and will be updated from time to time.

Users need to have authorized accounts and necessary permissions to access the hardware, software, and network facilities. They are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system, protect the privacy and work of users, and preserve the right to access the global networks to which the system is connected.

In case of complaints, appropriate action to be taken and will be decided by the ICT in-charge of the facility in consultation with the Principal/Competent Authority as appropriate.

1. Users with authorized accounts may use the computing and IT facilities for academic purposes, official Institute business, and for personal purposes so long as such use

- Does not violate any law, Institute policy or IT act of the Government of India.
- Does not interfere with the performance of Institute duties or work
- Does not result in commercial gain or private profit.

2. Users are expected to respect the privacy of other users and they must not allow any other person to use their password or share their account. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically and using passwords that are not easily guessed. Sharing of

passwords for any purpose is strictly prohibited. The user is responsible for any incident registered under his/her login identity.

3. Any attempt to circumvent system security, guess others' passwords, or in any way gain unauthorized access to local or network resources is forbidden. Users must not use another person's computing account, attempt to forge an account identity, or use a false account or email address.

4. Transferring copyrighted materials to or from the IIT campus systems without express consent of the authority is a violation of law. In addition, use of the internet for commercial gain or profit is not allowed. If done so, it will be sole responsibility of the concerned user.

5. Downloading of copyrighted movies/books/games/music/software via torrent's or other means is banned and may be tracked on receipt of any complaints. Any such activities will subject to disciplinary actions or punishment against the concerned user(s) as deemed appropriate by the Competent Authority .

6. No user shall at any time make available any data owned or generated by IIT Indore to others, which may lead to violation of the data sharing policy.

7. Downloading and Installation of unlicensed software on IIT facilities, or on individual machines connected to the IIT network or unnecessary download, is strictly prohibited.

8. It is forbidden to use email and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. It is also forbidden to send emails or messages masquerading as another person or to hide the sender's identity. Neither is any form of commercial advertising or soliciting allowed.

9. Spamming is strictly disallowed. Subscribing to mailing lists outside the Institute is an individual's responsibility.

10. Recreational downloads and peer to peer connections for recreational purposes are banned.

11. To the extent possible, users are expected to connect only to the premises Wi-Fi network (IITI_2.4GHz/5GHz or IITI) for wireless access. Setting up of unsecured Wi-Fi systems on the Institute network is prohibited.

12. It shall be responsibility of the user to log-out from the accounts after each use and shut- down the system properly. Abrupt shut-down by pulling off the plug is harmful and dangerous for the system and other installations.

13. It would be the responsibility of the user to protect his/her data and to take regular back-up since they would be working in de-centralized mode most of the time.

14. Users are expected to take proper care of equipment and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems. Any hardware change is not permitted to the users without prior permission from concerned authority.

15. No food or drinks are permitted in the computer laboratories. Also making noise either through games/ music or even talking and/ or singing loudly is prohibited.

16. Playing of Games or accessing recreational/offensive/pornography resources in Institute laboratories or by using Institute facilities is strictly prohibited.

17. Display of offensive material is strictly disallowed, and serious action will be taken against offenders.

18. Members who do not require continuation of services shall intimate the same in writing so that their accounts can be closed. It is compulsory for all users to get no-dues.

19. Violation of policy by users will be considered as misconduct and the concerned users will be barred from using internet. Further action may also be taken against the user(s) in case of serious IT offence as determined by Competent Authority.

20. The policy may change as and when it is considered appropriate and new policy or the changes in the policy will take effect immediately after the Circulation.

21. All Internet users/members accessing YouTube videos should restrict to only educational contents and avoid entertainment programs during and after official hours to have sufficient bandwidth for other users to complete the online official work.

Any activity which inconveniences users, depletes the computer resources, or jeopardizes the security of the systems, is considered as unethical use and will be taken seriously. Moreover, it should be noted that the action set out for various cases is not limited and can change.