



IIT Indore Email, IT Infrastructure and Network Usage Policy

IIT Indore Email, IT Infrastructure and Network Usage Policy

- This policy defines the acceptable use, access controls, and security requirements governing the Institute's IT infrastructure, network resources, and official email services at IIT Indore. It is intended to ensure secure, reliable, and efficient operation of IT services in support of academic, research, and administrative activities, while maintaining compliance with applicable laws and Government of India guidelines. All users are required to adhere to this policy, and any violations may result in disciplinary action as per Institute rules. The policy is subject to change and new policies or the changes in policy will take effect immediately after a brief announcement by any means (email, noticeboards, or official portals).

IIT INDORE EMAIL POLICY

This policy governs the use of official email services provided by IIT Indore to its faculty, staff, and students. It aims to ensure secure, efficient, and appropriate use of email communications within the institute. This policy helps keep IIT Indore's email system secure, efficient, and professional. It balances storage limits, security, and user convenience while maintaining compliance with government guidelines. The rules will be updated from time to time and the latest version of the rules will prevail.

1. Account Creation

- Every user at IIT Indore will be provided with an official email address with [@iiti.ac.in](mailto:iiti.ac.in) domain name.
- All active faculty, staff, and enrolled students are entitled to an official IIT Indore email account.

2. Storage & Access Management

- A limited storage space is provided to store your emails and attachments.
- Student accounts remain active until graduation, plus three months extra to migrate to alumni domain [@alum.iiti.ac.in](mailto:alum.iiti.ac.in).
- Employee accounts remain active as long as they work here, personal accounts will be deactivated after they leave.
- Role/Designation based account will be disabled till new person joins at same designation/role and then the same email/mailbox will be provided to new joinee.
- All emails in the mailbox in the Role/Designation based account should be safeguarded all the time. Deletion of past emails in Role/Designation based account is strictly prohibited to maintain the continuity of office related work/information.

3. Security

To keep your email safe and protect IIT Indore's systems, one must follow security rules.

- Usage of strong passwords is highly recommended.
- It is recommended to use two-factor authentication, which means logging in requires a password plus a code sent to phone or generated by an authenticator app.

4. Usage Guidelines

- The IIT email account is for official and academic purposes only.
- Email accounts must be used primarily for academic, research, and administrative purposes.
- Limited personal use is permitted, provided it does not interfere with official responsibilities or violate any policies.
- Sending mass emails (or unsolicited bulk emails) is not allowed to avoid spamming of inboxes.
- Don't forward official IIT circulars or notices to persons not concerned within or outside the institute without permission. Forwarding/sharing of official emails on social media websites is considered as violation of institute email policy.
- Don't store or share copyrighted or illegal content.
- Disseminating offensive, obscene, discriminatory, extreme political and ideological content is strictly prohibited.
- Engaging in activities that violate laws or institute policies is prohibited.
- Unauthorized use/ hacking of another individual's email account is not allowed.
- Forwarding/mirroring institute emails (especially those held by virtue of position as AR, DR, Head, Dean or Professor-in-Charge etc) is prohibited.
- **Emergency emails:** In case of emergencies like power outages or safety alerts, one can use priority tags to make sure your message is seen quickly.

5. Compliance & Monitoring

The IT department will regularly check email usage to ensure rules are followed.

- **Audits:** Email lists and storage usage will be reviewed from time to time.
- **Disciplinary actions:**
 - Breaking the rules can lead to disciplinary actions by the Institute which can include suspension of accounts or even termination of the accounts.
 - Individual users are ethically and legally responsible for what they post or write.
- **Legal disclaimer:** Emails sent and received on IIT Indore accounts are institute property and may be used as evidence if needed.

6. Account Management and Termination

- **Password Reset:** Users can request password resets through the IT helpdesk by providing necessary identification.
- **Mailbox Quota:** Mailbox storage is subject to limits as defined by the Institute. Users are required to proactively monitor and manage their mailbox usage, including periodic deletion or archival of emails. Reaching or exceeding the allotted quota may result in disruption of email services, including inability to send or receive emails. The system may not provide advance notifications, responsibility for compliance rests with the user.
- When the association with IIT Indore ends, the email account will be deactivated
- For students, only the important emails shall be transferred to their respective alumni IIT account after the graduation by themselves, so the regular account can be removed.
- After deactivation, anyone emailing you will get an automatic reply saying your message could not be delivered. After stipulated time of inactivity your account and data will be permanently deleted.

IT INDORE IT INFRASTRUCTURE USAGE POLICY

In its endeavour to provide all faculty, students, and staff with a modern, fully networked computing and IT environment for academic use, the institute has established the following IIT Indore IT Infrastructure Usage Policy.

1. General Usage

Faculty, staff, and students with authorized accounts may use the computing and IT facilities for academic purposes, official Institute business, and for personal purposes, provided such use:

- i. Does not violate any law, Institute policy, or the IT Act of the Government of India.
- ii. Does not interfere with the performance of Institute duties or academic work.
- iii. Does not result in commercial gain or private profit, unless explicitly allowed by the Institute.

2. Security and Access

- Circumventing system security, guessing passwords, or gaining unauthorized access is strictly forbidden. Do not use the Institute's computers to make unauthorized entries into any other computer or network.
- Users must not use another person's computing account or misrepresent their identity.
- Caution should be exercised while entering passwords on untrusted websites or responding to emails that impersonate admin, faculty or staff accounts.
- Do not take any actions that endanger the security of the IIT Indore network. Do not attempt to bypass firewalls or access controls. Do not set up any public servers (e.g., web, mail, proxy) that are visible outside the IIT Indore campus without approval from Dean IT (I&A).
- Use of VPN, proxy, tunnelling, or anonymization services like WARP, OpenVPN, Shadowsocks, etc to route Institute network traffic to external networks (inside to outside) is strictly prohibited. Any requirement for such access for academic or research purposes must be duly justified and approved by the concerned faculty member/Principal Investigator (PI). A formal request in the prescribed format, endorsed and signed by the PI, must be submitted to CITC for review and approval from Dean IT (I&A), prior to enabling such access.
- Use of unauthorized tunnelling or exposure tools is prohibited. Services such as ngrok, Cloudflare Tunnel, or similar tools that expose internal services to the public internet without approval are strictly not allowed, as they bypass institutional security controls. For hosting applications or sharing services externally, users shall use platforms such as Vercel, Netlify, etc.
- Use of anonymous or privacy-focused email services for official communication is restricted. Email services designed to provide anonymity (e.g., Proton Mail, Tutanota, etc.) must not be used for Institute-related communication or account registrations. All official correspondence must be conducted through Institute-provided email account to ensure accountability, traceability, and compliance with institutional policies.
- Respect the privacy of others when using any form of technology, including CCTV and the internet. Be aware of the purpose of CCTV cameras. They are often used for security, preventing vandalism, and monitoring for safety, not for general surveillance of individuals.

3. Copyright and Downloads

- Transferring copyrighted materials without the express consent of the owner is a legal violation.
- Use of the IITI internet facility for commercial gain or profit is not allowed.
- Downloading copyrighted content without the express consent of the owner via torrents or other means is prohibited and traceable. Fines and disciplinary actions may apply.
- Recreational downloads and peer-to-peer connections for recreational purposes are banned.
- Adhere to all legal protections for data and software, including copyright laws and software licenses. Do not use or distribute pirated software or infringe on intellectual property rights.

4. Software Installation

- Installation of new software on institute resources requires consent from the respective facility in-charge.
- Installation of unlicensed/pirated software is prohibited and will attract disciplinary action.

5. Network and Wi-Fi

- Users should connect only to official IIT Indore Wi-Fi networks.
- Setting up unsecured Wi-Fi access points is prohibited.

6. Content Filtering Rules

- Currently content filtering is enabled for some categories. These content filtering rules may be modified from time to time based on requirements and changes in usage policies. Any request for temporary/permanent relaxation on filtering rules will have to be recommended by concerned faculty/PI/Official and approved by the Dean IT (Infrastructure and Automation)
- Proper care must be taken of Wi-Fi access points provided in hostels, homes, and academic buildings.

7. VPN and SSH access to IITI LAN

- It is strictly prohibited to set up unauthorized VPN or ssh access facilities for connecting to IITI LAN from outside without explicit consent from CITC. The VPN facility available at CITC should be used for such purposes. It is also prohibited to facilitate external access to the IITI network using any terminal sharing or other similar software. The VPN facility is currently available to faculty, staff and students (on the recommendation of their supervisor).

8. Policy Violations

Generally, any user is violating policy if he/she is found misusing the Internet facilities via downloading of restricted or copyrighted content, security breach, hacking passwords of other users, sending inappropriate mails or any other activity which can be categorized as unethical.

- Violations will be treated as academic misconduct misdemeanour, or indiscipline as appropriate.
- Disciplinary actions may include warnings, fines, account suspension, or permanent revocation of access.
- Repeat or serious offenses will be handled by the appropriate Institute Committee.

General Advisory on Fair uses of Network, Internet, IT Resources and Email at IIT Indore

General Do's

1. Always follow the principle that "**what is not explicitly allowed is prohibited.**" This means that unless a specific action or usage is clearly permitted by the rules, it should be considered off-limits.
2. Limit your internet usage to essential activities. Excessive use can impact network performance and availability for others. Also Refrain from engaging in activities that consume excessive bandwidth, such as downloading large files or streaming high-definition videos during peak hours, to ensure fair usage for everyone.
3. Always verify the authenticity and validity of the information before using it for any purpose, especially for academic and professional matters. Ensure that any information you access on the internet is accurate and complete. Use reliable sources and double-check facts to avoid the spread of misinformation.
4. Adhere to all legal protections for data and software, including copyright laws and software licenses. Do not use or distribute pirated software or infringe on intellectual property rights.
5. Inform the Computer Committee /IT Department about any unusual occurrences or anomalies, such as potential security breaches or suspicious activities, to ensure a safe and secure network environment.
6. For any internet-related problems, contact IT department/IT Helpdesk. They are responsible for addressing and resolving technical issues related to internet access.
7. Use the internet exclusively for work-related or professional activities. Personal use should be minimal and must not interfere with academic or institutional priorities.
8. Periodically clean your browser history and cache to prevent slowdowns and maintain optimal performance. Regular maintenance helps in smooth browsing experiences.
9. Immediately delete any junk files or unwanted software that may have been accidentally installed. This prevents clutter and ensures efficient computer performance.
10. Always use rational judgment and act in the best interest of the Institute when accessing or downloading web content. Avoid accessing inappropriate or non-educational sites.
11. Ensure that your personal data and credentials are secure. Avoid sharing passwords and use strong, unique passwords for different accounts to protect against unauthorized access.
12. Install and regularly update antivirus software on your devices to protect against malware and other cyber threats. This is crucial for maintaining a secure computing environment.
13. You should login into any online institute meeting with valid username and/or any other role/designation-based credentials only.
14. You should strictly adhere to the decorum of joining an online meeting.
15. Follow all network policies and procedures established by the Institute. This includes compliance with any additional guidelines specific to certain departments or facilities.
16. If you find any ambiguities or have questions about the rules, reach out to the Computer Committee for clarification. Understanding the guidelines fully is essential for compliance.
17. Do visit <https://citc.iiti.ac.in/faqs/> for more information.

General Don'ts

1. Do not download files, images, videos, or songs that are large in size or contain inappropriate material such as pornography, racism, extreme political views, or content that incites violence, hatred, or any illegal activity.
2. Do not download content from the internet that is unrelated to your academic or professional work.
3. Do not download unlicensed/pirated software from the internet on the Institute's computers or any computer which is using Institute's network for Internet connectivity. Use only approved and licensed software to ensure compliance and security. Pirated software facilitate malware installation on computer and it's lateral spread, therefore causing security breaches.
4. Do not use end-to-end encrypted email services such as proton mail.
5. Do not use the Institute's computers to make unauthorized entries into any other computer or network. This includes hacking or attempting to gain unauthorized access.
6. Do not disrupt or interfere with other users, services, or equipment on the network. Intentional disruption of computer systems and networks is illegal. Do not reset or power off any machine/network element without proper authorization.
7. Do not represent yourself as another person in any form of communication or online activity. Do not deceive others about your identity in electronic communications or network traffic. Always provide accurate information about your identity.
8. Do not share your password with anyone. Keep your login credentials secure to prevent unauthorized access.
9. Do not leave your screen unattended. Always log out if you need to leave your computer to prevent unauthorized use.
10. Do not use the internet to transmit confidential, political, obscene, threatening, or harassing materials. Also, avoid sending content protected by intellectual property rights without permission.
11. Do not attach and transmit files or programs through email that contain illegal or unauthorized materials.
12. Do not contact anyone other than the designated contact persons mentioned in the guidelines for any concerns or issues.
13. Do not send emails to any community or group unless you have specific authorization to do so.
14. Do not tamper with network switches by removing or adding personal network cables, or use of access points (APs) for your own LAN setup. Any of such action will result in disciplinary action.

Privacy and Security Guidelines

1. Do not intrude on the privacy of others. Respect the confidentiality of personal information.
2. Do not attempt to access computers, accounts, files, or information belonging to others without their explicit knowledge and consent. Hacking or unauthorized access is strictly prohibited.
3. Do not take any actions that endanger the security of the IIT Indore network. Do not attempt to bypass firewalls or access controls. Avoid setting up any servers (e.g., web, mail, proxy) that are visible outside the IIT Indore campus.
4. Do not use IT resources to threaten, intimidate, or harass others. Respect the rights and dignity of all users.
5. Keep your provided computers updated with current virus detection software and the latest operating system updates. Regularly check for and remove viruses, worms, Trojan horses, and other malicious software.
6. Do not engage in illegal file sharing through internet or email. This includes the unauthorized distribution of copyrighted material.
7. Use your provided email ID for official communications only. Personal use should be kept to a minimum and must not interfere with institutional activities.
8. Please be advised that your institute email ID will be deactivated upon course completion / No dues completion. Therefore, avoid using it for personal purposes, including in research publications or any activities unrelated to the institute.
By following these detailed guidelines, you help maintain a secure, respectful, and efficient internet and email environment on campus.

Note:

1. All internet activity on the campus network is closely monitored and logged.
2. Every piece of material you access or download from the internet is automatically scanned for viruses and other malicious software.
3. All content you view or access on the internet is scanned for offensive material. This includes filtering out and blocking content that is deemed inappropriate.