



तमिलनाडुकेन्द्रीयविश्वविद्यालय  
(संसदद्वारापारितअधिनियम 2009 केअंतर्गतस्थापित)

**CENTRAL UNIVERSITY OF TAMIL NADU**  
(Established by an Act of Parliament, 2009)

नीलक्कुडीपरिसर/Neelakudi Campus, कंगलान्चेरी/Kangalancherry,  
तिरुवारूर/Thiruvarur- 610 005

**Information Technology Usage Policy**

**1. Title**

This policy can be called as Information Technology Usage Policy of Central University of Tamil Nadu, Thiruvarur.

**2. Definitions**

- a. "University" means Central University of Tamil Nadu, Thiruvarur.
- b. "IT Policy" means this policy and any amendments to this policy in future.
- c. "IT resources" means all the information technology resources and services including but not limited to computing, networking, communications and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, and any related materials and services.
- d. "User(s)" or "you" means every member of the University community including, but not limited to students, faculty members administrative officials, non-teaching staff, and independent contractors who use, accesses, or otherwise employs, locally or remotely, the University's IT resources, whether individually controlled, shared, stand-alone, or networked.

e. "Content" means any information, data, text, file, link, software, chat, pictures, video, communication and all that can be stored in a computer and posted on a webpage.

f. "User name" means any User name, login id, access id, screen name etc. that is used to identify a User and is used to access resources of this University.

g. "official email id" refers to the email id provided by the University to the individuals holding any academic and/ or administrative position of the University.

h. "group email id" means the email id that is created to communicate with any group of Users of this University.

i. "personal email id" refers to the email id provided by the University to the individual Users.

### **3. General policy statement**

This Policy Statement provides notice of Central University of Tamil Nadu, Thiruvavur expectations and guidelines that *is* applicable to all the Users. The University provides the IT Resources for the advancement of the University's growth with respect to its educational, research, and service objectives. Any access or use of IT Resources that interferes, interrupts, or conflicts with these objectives are not acceptable and will be considered as violation of this policy.

The University may at times sign contract with various software vendors or providers of other IT services. Such third party providers may provide their own policies that apply to Users. You are required to comply with such policies when using third party software or other IT services through the University's IT Resources.

Users accessing and using IT Resources are subject to this IT Policy in addition to applicable provisions of the University Statutes, University Ordinances, the Government of India Code of

Conduct, Student Handbooks, and all other policies and procedures established by the schools and administrative offices of the University.

### **3.1 User responsibilities**

The access and use of IT resources are limited to the purposes that are consistent with the instructional, academic, research, and administrative goals of the University and the User's relationship to those goals. Users are expected to uphold the standards and principles of the University while using the IT Resources. Accordingly, Users are required to respect the rights of others at all times.

Users are prohibited from using any portion of the IT Resources to post or transmit any information, data, text, file, link, software, chat, communication or other content that is harmful, abusive, discriminatory, hostile, combative, Threatening, insulting, embarrassing, harassing, intimidating, defamatory, Pornographic, obscene, or which negatively affects the University, another User, or any third party. Users who do not respect this spirit of use of the IT Resources may be held in violation of this IT Policy.

### **3.2 Usernames and passwords**

Using someone else's name or assuming identity without appropriate authorization, what so ever, is a violation of the University's principles and the IT Policy. University prohibits the use of any User name for the purposes of misrepresentation or as an attempt to avoid any obligations. All such unethical uses are prohibited by the University.

It is advisable to have individual passwords that shall meet the following criteria for better security and privacy:

- The password must be between 8 and 32 characters;
- The password must contain 1 numeric;
- The password must contain at least 1 uppercase and

lowercase character;

- The password must contain any of the following special characters:

~!@#\$%^&\*()\_+={}| \:”;<>,.?/.

Using different passwords for different accounts, changing passwords regularly and not writing the passwords on a paper or recording them on your email, mobile phones or files in your personal computer are some of the additional best practices.

### **3.3 Privacy**

Users should always note that, even when employing best practices, breaches can occur in any number of ways in the IT Resources or the User's own system(s). The best practices are only a precautionary measure to avoid breaches to their privacy. Accordingly, in addition to the provisions regarding privacy set forth, Users should not have an expectation of privacy in any content either located in the University's IT Resources or the User's own system, whether that content is protected by a User name and password or otherwise.

### **3.4 Compliance**

In consideration of the privilege of accessing and using the IT Resources, all Users must fully comply with the standards and responsibilities of acceptable use as outlined in:

1. All applicable provisions of the University Code of Conduct, employee handbooks and agreements, student handbooks and other policies and procedures established by various schools of the University;
2. All software license agreements acquired by the University and its authorized units;
3. This IT Policy in its entirety including the related policies: Anti-Spam Policy, Email Policy, Software usage and distribution policy; Peer-to-Peer Policy, Hosting Policy, Wireless Policy, and Internet Usage Policy;

4. All applicable University policies and procedures including, but not limited to, sexual harassment, academic dishonesty, scientific misconduct, and non-discrimination and this includes any standards or policy set for educational institutes by Govt. of India.

### **3.5 Respect to the rights of fellow Users**

The privilege of access of IT resources comes with the responsibility of respecting the rights and privacy of fellow Users and that includes the following:

- Respecting authorial integrity and the intellectual property rights of others;
- Respecting and protecting the integrity, availability, and security of all University IT Resources;
- Ensuring that all data and files that the User accesses or downloads are free from any computer code, file, or program which could damage, disrupt, expose to unauthorized access, or place excessive load on any computer system, network, or other IT Resource;
- Reporting any security risk or code, file, or program—including, but not limited to, computer viruses, Trojan Horses, worms, or any other "malware" - that infects any IT Resource including any owned or operated by the User; and
- Properly backing up appropriate User systems, software, and data.

### **3.6 Prohibited ways of access**

In addition to other prohibitions found in this IT Policy and any other applicable University code, statute, handbook, policy, or procedure, Users are

prohibited from accessing or using the IT Resources in the following manners or for the following purposes:

- Initiating or participating in unauthorized mass e-mailings to news groups, mailing lists, or individuals—including, but not limited to, chain letters, unsolicited commercial email, floods, and bombs;
- Giving others, by password or other means, any unauthorized access to any User account or the IT Resources, in whole or part;
- Seeking to, without authorization, deleting content, wrongly access, improperly use, interfere with, dismantle, disrupt, destroy, or prevent access to, any portion of the IT Resources including User or network accounts;
- Violating or otherwise compromising the privacy, or any other personal or property right, of other Users or third parties;
- Attempting to disguise the identity of the account or other IT Resource being used including, but not limited to "spoofing" resource addresses, impersonating any other person or entity, or misrepresenting affiliation with any other person or entity;
- *Using* the IT Resources to gain or attempt to gain unauthorized access to remote networks, including remote computer systems;
- Engaging in conduct constituting wasteful use of IT Resources or which unfairly monopolizes them to the exclusion of others;
- Engaging in conduct that results in interference

or degradation of controls and security of the IT Resources;

- Unless expressly authorized by the University in writing, exploiting or otherwise using the IT Resources for any commercial purpose;
- Engaging in cybercrimes or other prohibited acts as stated in the Govt. of India and State Govt. Laws;
- Knowingly or negligently running, installing, uploading, posting, emailing, or otherwise transmitting any computer code, file, or program—including, but not limited to, computer viruses, Trojan horses, worms, or any other "mal-ware"— which damages, exposes to unauthorized access, disrupts, or places excessive load on any computer system, network, or other IT Resource; and
- Using any IT Resource, including e-mail or other communication system to intimidate, insult, embarrass, or harass others; to interfere unreasonably with an individual's work, research, or educational performance; or to create a hostile or offensive working or learning environment.

#### **4. Intellectual Property**

All members of the faculty and student body have copyrights merely by authoring a paper whether for publication or even through a course assignment. Accordingly, as each User should have an expectation that others will not abuse his or her intellectual property rights, every User must also respect the intellectual property rights of others including those of other Users, all members of the University community, and all third parties. Hence, the University prohibits any copyright violation by Users knowingly or unknowingly within and outside the campus.

## **4.1 Violation of intellectual property rights**

*Any* violation of intellectual property laws and rights is not merely limited to unauthorized downloading of copyrighted music/movies/books through file-sharing software/illegal websites. Rather, the concept of intellectual property broadly covers all copyrighted works, trademarks, patents, and other proprietary and confidential information. Thus, intellectual property issues likely apply to any and all content that a particular User did not generate himself or herself and to which a User has not been given rights.

## **4.2 Potential Infringements**

Infringement of recorded music/movies/books, in various forms including but not limited to MP3/MOV/MPEG/MP4/FLV/DJVVU/PDF files, is a matter of concern to the University. The following uses are potentially infringing:

- Unauthorized broadcasting of copyrighted movies and videos for group of Users inside and outside the campus;
- Unauthorized copying of written works, including but not limited to textbooks and course materials;
- Unauthorized copying and use of digital videos or images, as well as logos and other marks;
- Unauthorized copying or installation of games or other software, including "shareware"; and
- Unauthorized copying or use of copyrighted, or otherwise proprietary, data or collections of data.

These are just a few examples of potential infringement that Users may intentionally or unintentionally commit.

It is the responsibility of every User to avoid infringing any intellectual property right and to report the infringement of another User if and when it is discovered. Failure to respect such rights, or report infringements, is a violation of this IT Policy and subject to the sanctions set forth below.



## 5. Privacy

All Users retain the right of privacy in their personal files and data, electronic mail, and voicemail as long as they are using the IT Resources in a manner consistent with the purposes, objectives, and mission of the University and this IT Policy. Likewise, Users are obligated to respect the right of privacy that other Users have in their own systems, data, and accounts.

Users should be aware that the University cannot guarantee security and \privacy during use of the IT Resources. To the contrary, various uses of the IT Resources or access in general, may not always be private. For example, issuance of a password or other means of access is to assure appropriate confidentiality of University-related information and files. However, it does not guarantee privacy in all cases, especially for personal or unlawful use of IT Resources.

University, in emergency situations, may also require backup and caching of various portions of the IT Resources; logging of activity; monitoring of general usage; and other activities that are not directed against any individual User or User account, for the purposes of emergency maintenance or restoring normal operations of the IT Resources.

In the event the University has reasonable suspicion that a User has violated any civil or criminal law, the University Code of Conduct, the IT Policy, or any other University policy, procedure, or regulation, the University reserves the right to access, inspect, monitor,

remove, take possession of, or surrender to civil or criminal authorities the offending Content, with or without notice or consent of the User. The University may also do so for the purpose of satisfying any law, regulation, or government request.

Further, the University may monitor the IT Resources to ensure that they are secure and being used in conformity with this IT Policy and other University guidelines. Thus, to the extent allowed by applicable law, the University reserves the right to examine, use, and disclose any data or content found on the University's IT Resources for the purposes of furthering the health, safety, discipline, security, or intellectual or other property of any User or other person or entity. Information that the University gathers from such permissible monitoring or examinations may also be used in disciplinary actions.

## **5. Monitoring, Reporting and Violations**

### **5.1 Monitoring**

As noted above, the University may, but *is* not required to, monitor, block, or otherwise prevent inappropriate use of the IT Resources. Nonetheless, in the event of a violation or failure to comply with this IT Policy, the University may monitor any User's access and use of the IT Resources in order to determine whether violations are taking place. If violations are found, the University may initiate charges and impose appropriate actions by following the various processes and procedural safeguards that are

applicable to the User's employment or enrolment status.

## **5.2 Reporting**

Users have an obligation to report violations of the IT Policy as well as any potential security or other breach of any portion of the IT Resources. Reporting of any such violations or other issues involving the inappropriate use of the IT Resources should be referred to:

- The Head of Department / Dean of Students/ Chief Warden if the alleged offender is a student;
- The concerned Dean or Vice Chancellor, if the alleged offender is a faculty member;
- Registrar, if the alleged offender is a non-teaching administrative staff.

## **5.3 Violations**

A violation of the IT Policy is considered a violation of the University's principles, objectives, and standards. Accordingly, in response to any given violation, the University may impose penalties ranging from the termination of the User's access to the IT Resources to disciplinary review and further action as necessary. In cases involving egregious violations like copying confidential papers from the administration; providing false information to the public/media; creating fake accounts on social networking sites that negatively affects the University or its members, etc., the University may institute legal action or cooperate with an action brought by applicable authorities or third parties.

The University will exercise good faith and proper discernment in its enforcement of the IT Policy. It will respect the academic freedom to which Users are entitled insofar as the legal rights and responsibilities of the individual User and the University

require. Failure to take action in any particular instance does not constitute an alteration of the IT Policy or a waiver of any right or remedy available to the University. Under no circumstance shall the University be liable to any User or third party for any violation including, but not limited to, illegal or improper acts, that any User commits through use of the IT Resources.

#### **5.4 User Obligation to Review**

Just as technology is constantly evolving, so are the policies that address it. Accordingly, the University will periodically update this IT Policy and it will be communicated to all Users. By accessing and using the IT Resources, each User represents and acknowledges that he or she has checked and read the updates in IT Policy on a regular basis so as to be informed of any changes hereto. If any User does not agree to check the IT Policy for revisions on a regular basis, said User may not use the IT Resources.

## **6. Email Usage Policy**

### **6.1 Email usage policy**

Email can be used as part of the electronic file processing in Government of India. Accordingly, University also uses email as an important part of communicating between members of University community. Hence, the Users are expected to be highly responsible while using the institute provided email accounts and the following points shall apply to all the Users of email.

- Every User is responsible for the mails received and sent from the email accounts provided to them by the University.
- The administration position holders avoid communicating official matters via their personal email ids. Similarly, any communication seeking permissions, clarifications or of official nature to any administrative staff of this University shall be addressed to the concerned official email id and not to their personal email id. It is the User's responsibility to know whom they are communicating to.

- Users are prohibited from sharing confidential information via email forwarding to any other emails including their individual email ids. They are also prohibited to share any confidential information to anyone to whom the email is not intended.
- Group email ids are meant to be used only for academic and other goals of the University and any other usage that is against this is prohibited.

## **6.2 Anti-Spam Policy**

Unsolicited commercial email, commonly referred to as "Spam", includes, but is not limited to, advertising email, bulk emails, email containing pyramid schemes, chain letters, emails containing unwanted questionable subject matter, and abusive or threatening email. Spam is often denoted by email that contains a false or misleading header, subject-line, identification of the sender, return address, routing or transmission path, or other false indication of origin, sometimes using a third party domain name without permission. In addition, Spam includes email that advertises goods or services that has been sent without the consent of the recipient, or without a pre-existing relationship between the sender and recipient.

The University wants to minimize the impact of Spam on the User community and IT Resources by implementing appropriate policies and technology. Users and third parties are prohibited from using the University's IT Resources to send Spam or to send any electronic correspondence in violation of this IT Policy or any applicable policy, law, rule, or regulation pertaining to unsolicited or bulk messages. The University reserves the right to refuse email or other connections from outside hosts that send any messages that appear to be unsolicited, meant for mass distribution, commercial in nature without prior approval of the intended User-recipient, prurient, offensive, or containing viruses, worms, or other malicious computer code. The University will use all available technology at its disposal to block such Spam.

### **6.3 Disclaimer for email**

All email communications via the institute provided email accounts are governed by necessary disclaimer policies of the University as mentioned in the University website.

## **7. Software Usage and Distribution Policy**

University tries to provide all the necessary software's for the conduct of teaching and research. This policy is concerned with all the software's used by any User of this University in the University created infrastructure like computers, smart phones, ipads, laptops, netbooks etc.,(hereinafter the "computers").

1. University purchases licenses for various software's from a variety of sources as approved by the Head/Dean/Registrar/Vice Chancellor (hereinafter the "Competent Authority"). Any pirated software or duplication of software except as permitted by related license agreements is prohibited. Users take full responsibility of the software's installed in the computers allotted to them.

2. Only software authorized by competent authority may be purchased, installed, or used on computers of the University. Personal software, or software that an employee has acquired for non-University purposes, may not be installed on University issued computers. The only software permitted for installation on University computers is authorized software for which University has been granted a license. In general any open source software that is used for research, teaching and learning and related academic/administrative works are authorized.

3. A copy of the software license must be provided to IT section for completion of registration and inventory requirements. Licenses must be registered in the name of Department/School/University and not in the name of an individual end-User. Any software procured by the University shall be registered under the name of the University.

4. Any software that is purchased with University's budget should be installed on a lab computer with access for other Users of this University,

unless authorized for use of an individual or a specific group. Such software's may be procured with necessary licences to be installed and used by multiple Users.

5. One of the best practices is to host software's like Matlab/ Mathematica/ Lingo/any other costly software at a common server (with appropriate licenses) and share it with the registered Users for that software resource.

## **8. Peer-to-Peer Applications**

Peer-to-peer applications like torrent clients, direct connect, WebRTC, SSH/FTP clients etc., are programs which allow computers to share data in the form of music, movies, games, or any computer file or software over a local network and the Internet without accessing a centralized distribution server or set of servers. The University does not, at this time, prohibit and does not block the use of peer-to-peer applications on any part of its network or the IT Resources. The University understands that there are legitimate academic uses for such applications. However, use of these applications has been known to cause problems which can affect the entire University community as well as individual Users.

The University expects that all IT Resources will be used in a manner consistent with the IT Policy and compliant with applicable laws. The University is under no obligation to protect a User from a complaint or action arising from any violation, or alleged violation, of the law, including infringement of any intellectual property right due to use of peer-to-peer, or any other type of "file-sharing," software or networks. Users should understand the fact that a material accessible through the University provided internet does not mean that accessing such material is authorized by third party rights-holders. In some cases, even content that is only accessible after a User pays for it may not be authorized for distribution by those who hold rights to that Content.

Accordingly, the University prohibits the use of peer-to-peer applications on its networks or the IT Resources, in general, to transmit or exchange any videos, music, software, images, or other Content, in which the

intellectual property is held by any party or entity other than the User, unless the User has valid, written authorization to access or distribute such Content. Any use of the IT Resources in violation of this policy will be subject to discipline or sanctions in keeping with the applicable provisions of the IT Policy and other University rules and policies. Nonetheless, the University allows and encourages the use of peer-to-peer applications for legitimate academic purposes when such uses do not involve any violation of applicable laws, or policies, or infringement of third party rights.

The University will endeavour to ensure that the User community is not adversely affected by the use of peer-to-peer programs. To that end, the University employs bandwidth management technology to make sure peer-to-peer programs do not degrade network speeds or any other portion of the IT Resources. Nonetheless, should such programs degrade the performance of the IT Resources, or otherwise affect them in a manner inconsistent with the IT Policy or other University policies, appropriate action will be taken against the User or Users responsible for such degradation or other negative impact.

Users should be aware that peer-to-peer applications are not necessarily harmless and using them, in addition to potentially degrading the IT Resources' performance, may:

- Violate copyright, patent, trademark, or other rights;
- May result in the disclosure confidential information; and
- May jeopardize the security of the IT Resources.

As noted above, disproportionate bandwidth usage and violation of applicable rights and laws constitute violations of the University's IT Policy. As such the practice of torrent downloads will be limited to open source software/operating systems which doesn't violate this policy. University may relax torrent downloads for other legitimate needs if approved by the competent authority.

## **9. Hosting WebPages**

"Hosting" is defined as providing network access to a site, or network accessible location, which provides distribution of Content. Hosting of such



distribution sites for entities other than University units, University affiliates, or registered student organizations (e.g., professional associations, consortiums, or journals) may be provided on University servers only when the entity has a relationship with the University that supports the University's teaching, research, or service mission. Such a relationship may be demonstrated by one or more of the following:

1. The entity is an organization of which the University itself is a member;
2. The entity is an organization of which a faculty or staff member is a member, and the appropriate University approves the hosting as being in support of the University's teaching, research, or service mission; and/or
3. The University has, or enters into, an authorized contractual relationship like MoU for hosting the entity's site.

The hosting of other distribution sites on or through the IT Resources by any User is strictly prohibited unless expressly authorized in writing by the University. This Hosting Policy, as part of the IT Policy, particularly applies to the hosting on or through the University's IT Resources of any website or other site or network access point accessed by other Users, or third parties from outside of the University community, which serves to distribute any Content through any number of networking protocols.

Thus, User setup and maintenance of distribution access points on the IT Resources that employ such protocols are violations of the IT Policy, unless otherwise provided for above. Such protocols include, but are not limited to, HyperText Transfer Protocol, File Transfer Protocol, Simple Mail Transfer Protocol, Internet Relay Chat Protocol, BitTorrent, Direct Connect Protocol or any other application layer protocols, now known or devised at any time hereafter, used to distribute Content, including the "secure" variations thereof.

## **10. Policy for Faculty WebPages**

University grants faculty members the right to create personal research- and teaching-focused sites within the limit of available resources. Access to the shared web server resources is a privilege, and it is provided with an expectation of responsible and acceptable use. Users who create personal web pages must follow all

our University policies including this IT and related policies, and state and Government laws.

Personal pages represent the views and opinions of their authors only. It is necessary to distinguish between the official department/school websites, which represent the University, and personal web pages, which may contain individual opinions and other content not related to the University. Your server account is for teaching and research purposes only. Your account can be suspended, and disciplinary action may be taken, if you use your personal site for commercial purposes.

### **10.1 Principles and Guidelines**

The specific principles and guidelines include, but are not limited to the following:

- Authorized Users are those individuals for whom the User name has been approved for this purpose. The User name and password combination is your identity and license to access and use the web server space for which you are specifically authorized.
- Authorized Users are responsible for the accuracy of the information published on their personal pages.
- University does not actively monitor or generally restrict the content of materials published on the faculty personal pages. However, the use of University resources is a privilege and not a public forum. Therefore, University reserves the right to restrict or deny usage of the web server space when such usage does not support the mission and vision of the University.
- All personal pages should include:
  - a. The author's name (e.g., "Created by: Author")
  - b. The 'last modified' date
  - c. A link to the University Personal Page Disclaimer.
- Users must adhere to legal and ethical standards governing copyright and intellectual property.
- That advocate hate, hostility, or violence, or contain offensive material, will be referred to the Vice Chancellor's Office for review.
- Be aware of privacy issues. Don't publish an individual's contact information or photo on your web site unless you obtain written

permission beforehand.

- Be respectful of other publishers' property. While it is easy to copy text, graphics, multimedia files, etc., from other sites, you must have permission from the copyright holder to use them on your personal site.
- Be mindful of the User. Avoid graphics that take too long to download. Avoid "under construction" pages; if you have any incomplete pages, don't publish them until you are ready. Avoid long, scrolling pages. Make effective use of links.

## **10.2 Personal Page Disclaimers**

The following disclaimer shall apply to all faculty web pages.

The views and opinions expressed on individual web pages are strictly those of their authors and are not official statements of the Central University of Tamil Nadu, Thiruvavur, India.

University does not actively monitor content published on individual pages. University recognizes the value of free speech but does not tolerate statements that advocate hate, hostility, or violence. If you feel any pages are in violation of this policy, contact [webmaster@cutn.ac.in](mailto:webmaster@cutn.ac.in).

## **11. Wireless Policy**

To ensure that all Users have fair and reliable access to the University's wireless networks, the University regulates this resource.

Accordingly, the University reserves the right to limit and restrict access to the wireless airspace on campus. Devices that may cause interference on the wireless network are prohibited.

Therefore, the wireless network on the University campus is monitored for interfering devices, such as smart TVs, wireless printers, and gaming devices. Accordingly, no User or other community member may install a wireless access point or any other device that interferes with the wireless network, on any University campus. Should any such

device be found, the University will notify the party of the issues concerned with the use of that device and require it to be removed and/or shut down.

The User Responsibilities and Statement of Prohibited Uses and other obligations and prohibitions found elsewhere in this IT policy, which govern the wired network portion of IT resources, also apply to the wireless network portion. Violations shall be handled in keeping with the guidelines set forth in the IT policy and other applicable statutes and policies.

## **12. Internet Usage Policy**

Social networking (e.g. maintaining an account or presence on the likes of Facebook, Myspace, etc.) and the posting of web-logs ("blogs") are increasingly popular forms of Internet usage. The University recognizes social networking and blogging as important means of self-expression and networking with people. However there will be a quota system that limits your internet usage for this purpose. Moreover, the University notes the educational and professional benefits of both.

Nonetheless, Users who use social networking and blogs should be aware of certain issues. Most social networking pages and blogs can be viewed, or even added to, by any User or third party having access to the Internet. Accordingly, the University cautions each User against posting Content that could divulge the User's private details or expose the User to embarrassment or ridicule. The University has no control over such potential disclosures by Users and, therefore, the University is not responsible for any such dissemination of private information.

The University reminds Users that, regardless of any efforts to the contrary, Users may be identified as members of the University community and therefore associated by third parties with the University. Accordingly, Users should remember that they are representatives of the University and should therefore comport themselves in accordance with the principles and standards of the University.

Moreover, every User should bear in mind that a potential employer, colleague, or other important business relation may review the User's posted Content anywhere on the Internet that is publicly accessible. As such, no User should falsely state or

exaggerate qualifications, accomplishments, affiliations, or other characteristics of either the User or the University.

*Users* should refrain from posting to social networks, blogs, or any other Internet site, any Content that may infringe any intellectual or other property rights of any other User or third party. The University disclaims any liability to User for User's posting or submission of Content on the Internet, through use of the IT Resources, regardless of type of action brought against User.

Lastly, the University notes that it does control the various third-party websites and other Internet destinations that Users access which are prohibited by the law. Accordingly, the University expressly disclaims any liability to Users resulting from any damage to any computing resources owned or otherwise controlled by Users including, but not limited to, hardware, software, or any peripherals.

University's Web Committee has all rights to recommend legal action against the individual / group who violate this IT Policy.

### **13. Forms:**

<b>Description</b>	<b>Download</b>
Wi-Fi User Registration Form	<a href="#">Click Here</a>
IP Address Requisition Form	<a href="#">Click Here</a>
Website Hosting Form	<a href="#">Click Here</a>