Policy for IT Resources
CHITKARA UNIVERSITY (CU)

IT Resources (internet/network/computer systems) usage

Need of policy:
Internet is an essential resource for institution users expect a certain level of performance and accessibility to academic resources. On the other hand, Internet access is a limited and expensive resource, and can easily be congested by uncontrolled and arbitrary usage. In addition, there are certain legal issues that arise when connecting the private network of the institution to the public Internet. Because of such reasons, it has been felt necessary to develop an Internet usage policy in compliance to Indian IT act 2000 and revised in year 2008 (http://deity.gov.in/content/cyber-laws), to streamline the internet service on the campus.

Guidelines for the users:

A. Internet/intranet resource is a privilege, not a right

University network and internet resource is a privilege, not a right of users which includes but not limited to all the employees of University/outsourced Staff/Visitors/all students etc. CU administration reserves the rights of logging/monitoring all activities in campus network/systems. Any type of hindrance created in the network will consider as the breach of this policy so nobody will/can cause damage to these resources willingly or unwillingly and even assist another in doing the same.

B. Acceptable usage

- It is mandatory for all staff/students/visitors to register their official/personal systems/gadgets with the Office of Information Technology (OIT).
- Access to the University network and internet services are provided for education and research purpose only for the staff and students.
- The above rules and expectations govern staff as well as students in usage of computers (and are applicable to other staff/students conduct and communication)
- Staff/students are further expected to comply with these rules and all specific instruction from the faculty or from their mentoring staff member/volunteer when accessing the University network resources (i.e. internet/intranet/computers/labs/laptops/tabs/gadgets etc.)

C. Disciplined Usage

- Respect other user’s use of IT resources and their privacy
- End users may/can not change IP’s issued static or via DHCP for PC’s/laptops on their own, any network service found interrupted due to this will be considered an offence.
- Material that would be considered inappropriate, offensive or disrespectful to others will not be accessed or installed/stored/configured on official as well as personnel systems/storage (i.e. desktops, portable HDD, pen drives, storage cards, laptops or hand held gadgets/tabs).
- Do not run/use tools/applications/services may cause interrupt/bandwidth override/hack campus systems/network (both inbound/outbound)
- Users must take adequate measures to prevent network misuse from computer systems that they are responsible.

issued: May 2013
• Reasonable care should be taken to minimize the vulnerability of systems attached to the campus network.
• Users should not upload/save/send University confidential and/or sensitive material to the public or any locations that are considered not appropriate or insecure.

D. Prohibited Usage

The user is responsible for his/her actions and activities involving University networks and internet services and for his/her computer files, passwords and accounts. Examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:
• **Accessing Inappropriate Materials** - Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegible.
• **Sharing Copyright Material** - Peer-to-peer (P2P) file sharing applications are often used to obtain copyrighted materials (e.g. music, movies, videos, text, software, applications etc.) without the permission of the owner/OEM or distributor while utilizing a disproportionate amount of network bandwidth and leaving the user’s computer vulnerable to computer viruses. It also violates applicable Indian Cyber Laws. **Examples** of P2P applications are BitTorrent, Gnutella, Limewire, eMule, Ares Galaxy, Kazzaa, Morpheus and Grokster. Therefore, the University has adopted the policy that P2P software, including those mentioned/exist above, would not be permitted to operate on its network.

**Powers of University Administration:**

• If there is any legal liability that ensues due to infringement of copyrighted material, CU will not be responsible for any liability and the person will be held responsible for this infringement. CU reserves the right, at its discretion, to review any student’s network access to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other University policies.
• Staff/students attempting to gain access using unauthorized tools/hardware, hacking other people’s systems, installing/storing pirated software, violating copyrights and plagiarism, misuse of official email, spamming etc.
• Accessing material via unauthorized proxies, using social sites/chatting/messaging during classes/online exams are offensive.
• Full internet access (without any restriction) will be given to only to authorized persons responsible for handling and managing the facility.
• The administration may monitor all internet usages. All internet activities can and will be logged for further review.
• The administration reserves the right to terminate any user’s access to the internet/intranet, at any time, which may violate the appropriate use of internet/intranet. In any violation of these rules & regulations, appropriate disciplinary action will be taken against the concerned user according to Indian IT Act 2000.

Compliance to internet user policy at all levels should be followed strictly. The IT policy has accorded the approval of Hon’ble Vice Chancellor.