Internet Access, E-Mail, Use of Software and Hardware Maintenance Policy

It has become very essential to enact a useful ICT policy for the following reasons:

i. To ensure smooth operations of ICT infrastructure and access to internet

ii. To protect its vital information like exam results data, accounts data etc. from unauthorized access

iii. To make available minimum internet bandwidth to each academic user to ensure the high availability of academic e-resources

iv. To standardize the ICT procurement and maintenance process

v. To enforce and ensure minimum information & network security standards to prevent any misuse from its own users and outsiders

vi. To protect its ICT infrastructure from cyber-attacks and to prevent it from being used as a platform to create a cyber-attack somewhere outside the campus

1. All users should be aware that several network usage issues are covered by the Indian IT Act 2000 and IT Amendment Act 2008, violation of which is an offence under national law.
2. Do not download content(s) from Internet sites unless it is related to your work.
3. Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.
4. Do not forget to log out when left unattended for more than 5 mins, to prevent any misuse.
5. Do not attach and transmit files (or programs) through email which contains illegal/unauthorized materials.
6. Faculty, staff, and students with authorized accounts may use the computing and IT facilities for academic purposes, official University business, and for personal purposes so long as such use:

   a. Does not violate any law, University policy or IT act of the Government of India

   b. Does not interfere with the performance of Chaudhary Ranbir Singh University, Jind duties or work of an academic nature.

   c. Does not result in commercial gain or private profit other than that allowed by the Chaudhary Ranbir Singh University, Jind.

7. Users are expected to respect the privacy of other users and they may 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 whatsoever is strictly prohibited. Users may share the required files through sharing software with proper Access Control List (ACL).
8. Any attempt to circumvent system security, guess others' passwords, or in anyway gain unauthorized access to local or network resources is forbidden. Users may not use another person's computing account, attempt to forge an account identity, or use a false account or email address.
9. Transferring copyrighted materials to or from the Chaudhary Ranbir Singh University, Jind systems without express consent of the owner is a violation of international 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 user.
10. Downloading and installing of new software has to be done with the explicit consent of the respective facility in-charges. Installation of unlicensed software on Chaudhary Ranbir Singh University, Jind facilities, or on individual machines connected to the CRSU network, is strictly prohibited.
11. To the extent possible, users are expected to use only their official email addresses provided by Chaudhary Ranbir Singh University, Jind for official communications with other members of the University.
12. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. Neither is any form of commercial advertising, or soliciting allowed. Spamming is strictly disallowed. Subscribing to mailing lists outside the Institute is an individual's responsibility.
13. Shared email accounts for any purpose whatsoever are not allowed. Any special accounts, if need to be set up for conferences and other valid reasons as determined by the university authorities, must have a single designated user.
14. Recreational downloads and peer to peer connections for recreational purposes are not allowed unless it is academic requirement.
15. To the extent possible, users are expected to connect only to the official Chaudhary Ranbir Singh University Wi-Fi network for wireless access. Setting up of unsecured Wi-Fi systems

on the Chaudhary Ranbir Singh University network is prohibited in accordance with Government of India guidelines.

16. Users are expected to take proper care of network equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility.
17. Playing of Games & watching movies in University laboratories/University terminals or using University facilities for same is strictly prohibited.
18. Display and storage of offensive material like storing pornographic material on the disk, viewing pornographic material on the terminals is strictly disallowed and serious action will be taken against offenders.
19. Wasting of resources like unnecessary downloads from Internet , giving accounts to other persons, sometimes outsiders, using personal account to do outside work for which the individual is paid are not allowed.
20. Security related misuse like breaking security of systems, trying to capture password of other users, damaging/gaining access to the data of the other users is taken most seriously.
21. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the university authorities may fine/or and take an action by issuing a warning through disabling the access. In extreme cases, the access to the network may be completely disabled to IT facilities at Chaudhary Ranbir Singh University, Jind, and/ or sent to the University authorities.
22. Any part/component of the ICT infrastructure of the university shall not be misused for Anti-University, Anti-State or Anti-Government activities. The University Computer and Informatics Centre (UCIC) will be authorized to undertake appropriate measures to ensure maintenance of such discipline and initiate suitable actions for preventions of such undesirable activities.
23. All communication though E-mail can be authenticated if sent through crsu.ac.in implying that all other mails sent through other domains may not be considered official and no action can be taken on that.
24. The University Computer and Informatics Centre (UCIC) has the right to monitor and scan all information carried by the network for the purpose of detecting and identifying inappropriate use. As such the privacy of information carried by the network is not guaranteed. University Computer and Informatics Centre (UCIC) is authorized to break open a PC or disconnect it from the network, if called for. However, specific scanning will be done only on approval / post facto approval by a competent authority. This is in accordance with the Indian IT Act 2000.

Khatker

25. User department must be vigilant about warranty checks and after the completion of the warranty period, User Department may implement the Annual Maintenance Contract (AMC) for the device/equipment depending on the criticality of its usage, with the approval of the competent authority & following the standard procedure laid down by the university from time to time.
26. Access to sites that are banned under law or that are offensive or obscene is prohibited. This is also an offence under the Indian IT Act 2000 and attracts severe punishment.
27. Use of the network to tamper with information on other computers, to deliberately spread harmful/pirated programs, compromise other systems, or to cause damage of any kind using the intranet/internet is prohibited, and is an offence under the Indian IT Act 2000. The user is liable for any civil losses caused, in addition to criminal prosecution under the Indian IT Act 2000.
28. The user department where the ICT equipment is installed and used, either temporarily or permanently, is responsible for the physical security of it and It is responsible for allowing the physical access to the ICT resources only to authorized users.
29. It is also responsible to ensure proper power supply with effective grounding (earthing), proper furniture as well as cleanliness of the equipment and environment including air-conditioning machines.
30. Individual users as well as User departments should take reasonable care of the vulnerability of systems attached to the campus network. In particular, users must apply appropriate service packs, browser updates and antivirus and client security solutions in their MS Windows machines, and necessary upgrades, OS patches, browser updates etc. for other systems.
31. If a user department wishes to set up its own Internet access facility, then it should be done under support and monitoring of the University Computer and Informatics Centre (UCIC) and ensure that deploying such an access facility does not jeopardize the security of the campus network. The user department must completely adhere to the provisions of this ICT Policy for such facility.
32. Software programs are covered by copyrights and a license is required for their use.
33. Users / User departments must ensure that they have either an academic, commercial or public license (as in the case of 'free' software) for any software they install on the systems that they are responsible for.
34. Use and exchange of pirated / illegal software over the CRSU is prohibited. It is the responsibility of the head of the user department to ensure compliance.

35. The downloading and use of software that is not characterized as public domain or 'free' is prohibited.

36. Use of Open Source Software is encouraged to avoid financial burden and legal complications arising out of license management. For example, use of Kingsoft Office Or Open Office must be preferred over MS-Office, Thunderbird E-Mail Client as against MS Outlook.

ASf Khatker