पंजाब केन्द्रीय विश्वविद्यालय/ਪੰਜਾਬ ਕੇਂਦਰੀ ਯੂਨੀਵਰਸਿਟੀ

Central University of Punjab

A Central University established by an Act of Parliament

Policy for Information and Technology

PREAMBLE

The purpose of this policy is to ensure the legitimate and optimal use of IT resources at the university. The aim of the policy is to facilitate the safe, secured, effective, target oriented and lawful use based on spirit of co-operation and sharing in pursuance of Vision Statement of the university. The policy shall cover all Information Technology facilities and services provided by CUP. It shall regulate the use of ICT resources by all the stakeholders and IT facilities & information resources shall be the property of the University and not of a particular individual, School or Centre.

Scope of Application

This policy shall be applicable for the use of information, electronic devices, computing devices, and network resources of the university. All students, employees, consultants, and other workers at university are responsible for exercising rational judgment regarding appropriate and judicious use of ICT infrastructure in accordance with the following:

- IT Act 2000 including all subsequent Amendments
- E-mail Policy of the Government of India
- Any other policy or guidelines issued by the Government of India from time to time

NOTE: In addition to above, the university can also devise guidelines for the expansion and use of ICT infrastructure. Such guidelines shall be open for amendments, as and when required.

Date of Commencement

This policy shall be brought into force from the date of its approval by the statutory bodies of the University.

Definition of Clause

Unless the context requires otherwise, the expression defined hereinafter shall be construed in following sense:

1. IT Resource : The expression IT resource shall include the computer equipment/s, portable and mobile devices, and facilities including the network-internet and intra-net, wireless networks, external storage devices, peripherals like printers and scanners and the software associated therewith and available at any point of time along with the information and data generated for official purpose and all electronic information and communications contained on the network

2. **Network Resource:** It shall include any electronic/electrical and/or mechanical devices connected to computer network of the university

3. **Users:** It shall include all students, employees, consultants, and any other person permitted by the Competent Authority for using IT Resources/facilities at the university

4. **Malicious Program:** It includes software that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious codes

5. **Disruption:** It means a circumstance or event that interrupts or prevents the correct operation of system services and functions

6. **Blog:** A discussion or informational site published on the World Wide Web

7. **Competent Authority:** The expression in reference of Section 3 shall stand for statutory body and for section 4.3, it shall be any official designated for the above-said purpose.

Proprietary Information It shall include any data, information that has been the part of official assignment and a password of resource, if any

8. **Proprietary Information:** It shall include any data, information that has been the part of official assignment and a password of resource, if any

General Use, Access to Network and Ownership

The proprietary information of the University stored on electronic and computing devices whether owned or leased by the university, the employees, and students or a third party remains the sole property of Central University of Punjab.
The users of IT facilities and services of university shall be responsible to promptly report the theft, loss or unauthorized disclosure of the University's proprietary information.
The users shall access, use or share CUP proprietary information only to the extent it is authorized and necessary to complete the assigned job related responsibilities.

For connecting to CUP wireless, the user shall ensure the following:
(a)A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the wireless network.
(b)Wireless client systems and wireless devices shall not be allowed to connect to the wireless access points or remote network without due authentication.
(c)To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.
(d)The users shall be allowed to remotely access the services and resources of the University by adhering to the procedure to be notified and specified by the competent authority from time to time.

Filtering and Blocking of Sites

1.The university, through its Competent Authority may block content on the Internet by issuing a circular, which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or policy of the University or which may pose a security threat to the network or undermine the interests of the university.
2.The university may also block content which, in the opinion of the Competent Authority, is inappropriate or may adversely affect the productivity of the users.

Security and Password

1. All IT resources shall be secured by strong password including document as well as equipment password. The password should include a combination of lowercase & uppercase alphabets, numerical and special characters.
2. All computing devices shall be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. The screen must be locked or logged off when the device is unattended.
3. PC shall not be left unattended without logging off and the user shall be responsible for any misuse of such a device by unauthorised access.
4. The users shall exercise utmost caution while opening an e-mail attachments received from unknown senders, which may contain malware.

5. The users shall be responsible for all activity performed with their personal user ID and/or passwords. Permitting any other person to perform any activity with one's user ID and/or passwords shall be permissible with prior written approval from the competent authority with an undertaking that such a password shall be subsequently changed. These shall be treated as sensitive and confidential information.
6. No official of the University shall require, for whatever purpose, the password of other officials on any kind of questionnaire, in writing or oral, through phone or electronic message service unless permitted by the competent authority in writing with an undertaking that such a password shall be subsequently changed.
The users shall refuse all offers by the software to place a cookie on their computer so that they cannot automatically log on the next time when they visit a particular Internet site

Electronic Monitoring

1.The university shall have the right to audit networks and systems at regular intervals, for ensuring compliance of the policy in the case of a specific alleged misconduct or to redress any fault in the functioning of the system. However, this can be done on the prior approval of the competent authority and under intimation to the user.
2.The university or any person authorized on its behalf, for security related reasons or for compliance with applicable laws, may access review, copy or delete any kind of electronic communication or files stored on the devices under the possession of the university by adopting the following procedure:
(a)The user must be intimated.
(b)If found necessary to access or inspect any device without intimation to its user, it can only be done with the prior approval of the competent authority.

Unauthorized access

Any unauthorised access to any system or its part/s, information or facilities shall be strictly prohibited and invoke disciplinary action.

Unacceptable Use

Under no circumstances, a user of IT resources and facilities of the University shall be authorized to engage in any activity that is illegal under Indian or international law.
Following activities shall be prohibited in general. In case, the need arises, select users can be exempted from these restrictions. This list is however not exhaustive, but it provides a basic framework of activities falling into the category of unacceptable usage.

System and Network Activities

- The users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the university.
- Any infringement of copyright materials including, but not limited to, digitization and sharing of photographs from magazines, books or other copyrighted sources/Movie/Music, and the installation of any copyrighted software for which university or the end user does not have any active license.
- Accessing data, a server, an account or any IT equipment for any purpose other than academics, research and official work related to the university.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Sharing account password with others or allowing use of account by others including family members while working at home.
- Using computing asset of the University to actively engage in procuring or transmitting material that is in violation of sexual harassment/ Human Rights or material considered hostile at the workplace.
- Making fraudulent offers of products, items or services originating from any university account.
- Making statements about warranty, explicitly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches including, accessing data for which the user is not an intended recipient or logging into a server or account that the user is not authorized to access, unless these duties are within the scope of regular duties. For the purpose of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which shall intercept data not intended for the user's host, unless this activity is a part of the user's normal job responsibility.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honey nets, or similar technology on the University network.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or the Internet/Intranet/Extranet.

Electronic Monitoring

While using university IT resources to access and use the Internet, following points are to be adhered to:

1. The users must realize that they represent the University. Whenever users state an affiliation to the University, they must also indicate that "the opinions expressed are my own and not that of the university".

2.E-mail service authorized by the university shall only be used for all official correspondences after the specific notification as to the implementation of this Clause.

3.For personal correspondence, users may use the name-based e-mail id assigned to them on the university authorized e-mail Service.

The following activities are strictly prohibited:

1.Sending unsolicited email messages, including junk mails or other advertising material to individuals who did not specifically request for such materials (email spam).

2.Any form of harassment via email, telephone, whether through language, frequency or size of messages.

3.Unauthorized use or forging of email header information.

4.Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5.Creating or forwarding "chain letters", or other "pyramid" schemes of any type.

6.Use of unsolicited email originating from within the network of the University or from other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CUP or connected via network of CUP.

7.Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

8.Retiring or the employees being relieved and the students leaving the university shall surrender the mail Id allotted on CUP domain name or CUP email server for clearing their No Dues.

Blogging and Social Media

In contrast to other traditional media, social media is more interactive, enables one-to-one conversation and facilitates instant response. However, the University is aware of the fact that on such platforms the perception of an official and personal roles and boundaries is often blurred. Therefore, while using social media for official purposes, the following may be kept in mind to smoothen interaction. An official Blogging or access to social media will be regulated by the administrator. Limited and occasional use of the systems of CUP to engage in blogging is acceptable subject to the conditions specified hereinafter.

1.Social Media can be accessed only after office hours. If a user is required to use it for a part of his official assignment or collecting any information during office hours, it can be permitted by the competent authority.

Exception Following shall be exempted from the application of this rule:

(a) Users or any other official working for the Department of Public Relations.

(b) Users or any other official working for community outreach under the Community Outreach Programme.

2.There shall be absolute prohibition on the users for making any discriminatory, disparaging, defamatory or harassing comments or bullying while blogging or using social media. The acts, omission or any statement resulting into instigation, abatement to commit any offence, creating communal hatred or apathy shall be strictly prohibited.
3.No user shall involve oneself in any kind of blogging resulting into compromise with the interests of the university including its employees.
4.No user shall attribute one's personal statements, opinions or beliefs while using university network while engaged in blogging or accessing social media.
5.Apart from following all laws of the land pertaining to peace and order as well as the handling and disclosure of copyrighted or export controlled materials, the logos of CUP and any other CUP intellectual property shall also not be used in connection with any blogging activity.
6.Core Values for Users of Blogs and Social Media:
(a)Identity: In official communications, user must reveal his identity and his role in the department and publish in the first person. Disclaimer may be used when appropriate.
(b)Authority: Users shall not comment and respond unless authorized to do so especially in any of the following matters:
i.Recruitment
ii.Examinations
iii.Tenders
iv.Quotations
v.Subjudice matter
vi.Draft Rules, Regulations, Notifications, Circulars
vii.Injuring and damaging the reputation of any staff and the student and also the university.
(c) Relevance: The users can comment on issues relevant to their area of specialisation and make relevant and pertinent comments without compromising the interest of the university. This will make conversation productive and help in taking it to its logical conclusion. However, the university shall not take any responsibility for any of such comments and it must be ensured by the user before making any comment or participating in the deliberation that the comments or ideas expressed by her/him are their personal ones, and not of the university.
(d) Professionalism: The users must be polite, discrete and respectful to all. They shall refrain themselves from making any personal comments for or against any individuals or agencies. They should be careful not to politicize any kind of professional discussions.
(e) Compliance: The users shall be compliant to relevant rules and regulations. They should not infringe upon IPR.
(f) Privacy: Personal information about other individuals as well as one's own private and personal details shall not be revealed unless these are meant to be made public.

Dissemination of IT Policy

For dissemination, following measures shall be adopted:
1.Mandatory disclosure of policy on the university Website.
2.Orientation sessions at the time of joining of employees and students to the university.

Disciplinary and Legal Measures

1. Deliberate breach of the provisions contained in this policy statement, shall invoke disciplinary action which may include, in addition to the penalties, denial of access to IT services and facilities offered by the university. On the other hand, if the act is covered with the meanings and definitions of offences defined under Indian Penal Code, 1860, Information Technology Act, 2000 (with Amendments) and any other allied laws, regulations, the legal proceedings against the person in conflict with policy or offender shall be initiated within the prior written approval of the Competent Authority.
2. Notwithstanding the above, the Competent Authority shall have the Authority to take appropriate action in case any act is not covered under the provisions referred here-in-before if the act or omission affects national interest, interest of the university or proves otherwise offensive.

Annual Budget

On the recommendation of In-charge of the Computer Centre, annual budget shall be allocated for the maintenance and upgradation of the ICT infrastructure for smooth and improved functioning.

Power to Revise

This IT Policy shall be subject to revision by the university from time to time.

Power to Remove Difficulty

If any difficulty arises while implementing this policy, the competent authority can take appropriate decision to remove the same.

For any query, please contact:
Internal Quality Assurance Cell
आतंरिक गुणवत्ता सुनिश्चयन प्रकोष्ठ
Central University of Punjab
पंजाब केंद्रीय विश्वविद्यालय
Bathinda - 151 401
भटिंडा - 151 401
Email: iqacoffice@cup.edu.in
: