Annexure-XXIII

CUPB IT POLICY

1. Aim and Objective Statement:

The purpose of this policy is to sketch out the acceptable and ensure the legitimate use of IT resources at Central University of Punjab (CUPB). All CUPB's IT facilities and information resources shall be the property of the University and not of a particular individual School or Centre. The aim of the policy is to facilitate the safe, secured, effective, target oriented and lawful use based on spirit of co-operation in pursuance of Vision Statement of CUPB.

The policy shall cover all Information Technology facilities and services provided by CUPB. It shall govern the use of resources of information technology by all the stakeholders of CUPB.

2. Scope of Application:

This policy shall apply to the use of information, electronic devices, computing devices, and network resources of CUPB. All students, employees, consultants, temporary, and other workers at CUPB and its subsidiaries are responsible for exercising rational judgment regarding appropriate and judicious use of information, electronic devices, and network resources in accordance with followings:

- IT Act 2000 and its Amendment.
- Email Policy of the Government of India.
- Any other policy or standards issued by the Government of India from time to time.

Note: The above rules shall apply *with necessary modifications (mutatis mutandis)* to the users of CUPB network.

- Policies and standards issued by CUPB which shall be subject to modification from time to time.

3. **Date of Commencement**: This policy shall be brought into force from the date of its approval by the statutory bodies of the University.

4. **Definition Clause:** Unless the context requires otherwise, the expression defined hereinafter shall be construed in following sense-

   4.1 **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 in addition to information and data generated for official purpose and all electronic information and communication contained on the network.

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

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

4.4 **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 logic.

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

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

4.7 **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.

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

5. General Use, Access to Network and Ownership:

5.1 The proprietary information of CUPB 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.

5.2 The users of IT facilities and services of university shall be responsible to promptly report the theft, loss or unauthorized disclosure of CUPB proprietary information.

5.3 The users shall access, use or share CUPB proprietary information only to the extent it is authorized and necessary to complete the assigned job responsibilities

5.4 For connecting to a CUPB wireless, 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 CUPB wireless network.

(b) Wireless client systems and wireless devices shall not be allowed to connect to the CUPB 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 CUPB by adhering the procedure to be notified and specified by the competent authority from time to time.

6. Filtering and Blocking of Sites:

6.1 CUPB, through its Competent Authority by issuing a Circular about the information, may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or policy of CUPB or which may pose a security threat to the network or undermine the interests of CUPB.

6.2 CUPB may also block content which, in the opinion of the Competent Authority, is inappropriate or may adversely affect the productivity of the users.

7. Security and Password:

7.1 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.

7.2 All computing devices shall be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

7.3 No PC shall be left unattended without logging off and the user shall be responsible for any misuse of such a device.

7.4 The users shall use extreme caution while opening e-mail attachments received from unknown senders, which may contain malware.

7.5 Users shall be responsible for all activity performed with their personal user ID and/or passwords. Users shall not permit others to perform any activity with their user IDs and/or passwords or perform any activity with IDs and/or passwords belonging to other users. 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.

7.6 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.

7.7 Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

8. Electronic Monitoring:

8.1 CUPB shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy in the case of a specific alleged misconduct or to redress any fault in the functioning of the system.

Provided that above access shall be lawful only with the prior approval of competent authority and under intimation to the user.

8.2 CUPB 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 CUPB provided devices by adopting the procedure given below:

(a) The user must be intimated.

(b) Should such access be necessary without seeking the user's permission, it should, wherever possible, be approved by a competent authority prior to inspection.

(c) If it has not been possible to intimate the user, any access should be reported to the user or to an appropriate authority as soon as possible.

9. Unauthorized Access: Access to any system or its part/s, information or facilities shall be strictly prohibited and invoke disciplinary action.

10. Unacceptable Use: Under no circumstances, a user of IT resources and facilities of CUPB shall be authorized to engage in any activity that is illegal under Indian or international law.

Following activities shall be, in general, prohibited but the authorized users shall be exempted from these restrictions during the course of their legitimate job responsibilities. The lists below are by no means exhaustive, but this is an attempt to provide a framework of activities falling into the category of unacceptable use.

10.1 **System and Network Activities:**

(a) 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.

(b) 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 CUPB.

(c) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CUPB or the end user does not have an active license.

(d) Accessing data, a server, an account or any IT equipment for any purpose other than academics, research and official work related to CUPB.

(e) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.

(f) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(g) Revealing your account password to others or allowing use of your account by others including family and other household members while working at home.

(h) Using a CUPB computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

(i) Making fraudulent offers of products, items, or services originating from any CUPB account.

(j) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

(k) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes 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.

(l) Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job responsibility.
(m) Circumventing user authentication or security of any host, network or account.
(n) Introducing honeypots, honey nets, or similar technology on the CUPB network.
(o) 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 via the Internet/Intranet/Extranet.

11. Email and Communication Activities:

While using CUPB IT resources to access and use the Internet. Following points are to be followed:

11.1 the users must realize that they represent CUPB. Whenever users state an affiliation to CUPB, they must also indicate that "the opinions expressed are my own and not necessarily those of the CUPB ".

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

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

The following activities are strictly prohibited:

11.4 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

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

11.6 Unauthorized use or forging of email header information.

11.7 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.

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

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

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

11.11 Retiring or the employees being relieved and the students leaving the university shall surrender a mail Id allotted on CUPB domain name or CUPB email server before clearing their No Dues Certificate.

12. 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, CUPB is aware of the fact that on such platforms the perception of 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. Blogging or access to social media is regulated. Limited and occasional use of systems of CUPB to engage in blogging is acceptable subject to the conditions specified hereinafter.

12.1 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.

12.2 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.

12.3 No user shall involve oneself in any kind of blogging resulting into compromise with the interests of the university including its employees.

12.4 No user shall attribute one's personal statements, opinions or beliefs to Central CUPB when engaged in blogging or accessing social media.

12.5 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 CUPB and any other CUPB intellectual property shall also not be used in connection with any blogging activity.

12.6 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. Matter sub-judice (pending);
vi. Draft Rules, Regulations, Notifications, Circulars;
vii. Injuring and damaging the reputation of any Colleague, student and CUPB.

(c) Relevance: Users can comment on issues relevant to their area and make relevant and pertinent comments without compromising the interest of the CUPB. This will make conversation productive and help take it to its logical conclusion. However, CUPB shall not be responsible for any comments and it must be ensured by the user before making any comment or participating in the deliberation that the comments or idea expressed by him are his personal, not representing CUPB.

(d) Professionalism: 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: Users shall be compliant to relevant rules and regulations. They should not infringe upon IPR, copyright of others.

(f) Privacy: Do not reveal personal information about other individuals as well as do not publish your own private and personal details unless you wish for them to be made public to be used by others.

13. Dissemination of IT Policy: For dissemination, following measures shall be adopted:

13.1 Mandatory disclosure of policy on the CUPB Website.

13.2 Orientation session at the time of commencement for all Stakeholders.

13.3 One session during Orientation Programme for newly admitted students or all recruited Staff.

Disciplinary and Legal Measures:

13.4 Deliberated and serious breach of the policy statements in this section shall invoke disciplinary measures which may include, in addition to the penalties, person in conflict with policy/offender being denied access to IT services and facilities offered by CUPB. Nonetheless, 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.

13.5 Notwithstanding discussed above, the Competent Authority shall have the Authority to take appropriate action in case any act is not covered under the provisions referred hereinbefore if the act or omission affects national interest, interest of the CUPB or proves otherwise offensive.

14. Power to Revise: The rules under this IT Policy of CUPB shall be subject to revision by the Competent Authority from time to time.