UNIVERSITY OF CALCUTTA

87/1, College Street, Kolkata - 700 073

Adhoc Network and Internet Use Policy

The University uses computers as one way of enhancing its mission to teach the skills, knowledge and behaviour's. Computers provide unequalled opportunities to explore and use a varied and exciting set of resources. In order to make these resources available to everyone, those who use the University's available technology must do so in a way that is consistent with their educational mission.

These rules are intended to provide general guidelines and examples of prohibited computer and Internet uses, but do not attempt to state all required or prohibited activities by users. Failure to comply with the *University of Calcutta Network and Internet Use Policy* and these rules may result in loss of computer and Internet privileges, and/or legal and disciplinary action.

A. Network/Internet Use is a Privilege, Not a Right

Staff/Student use of the University networks and Internet services is a privilege, not a right. No person will deliberately or wilfully cause damage to computer equipment or assist another in doing the same. Unacceptable use/activity may result in suspension or cancellation of privileges as well as additional disciplinary action and/or legal action. **The Internet Committee** shall have final authority to decide whether a staff/student's privileges will be denied or revoked.

B. Acceptable Use

Staff/Student access to the University networks and Internet services are provided for educational purposes and research consistent with the University's educational mission, curriculum and instructional goals. The same rules and expectations govern staff/student use of computers as apply to other staff/student conduct and communication. Staff/Students are further expected to comply with these rules and all specific instructions from the Faculty or to his/her supervising staff member when accessing the University networks and Internet services.

University staffs, students, and guests have shared access to wireless network resources to support the University's mission of teaching, research and outreach. Any wireless network device that would extend the University network and is not managed by the authoritative campus network will be considered a rogue device and will be subject to detection and immediate removal from the network

Authorized users of the University network are responsible for knowing and adhering to user rights and responsibilities as defined in Administrative Policy.

The users behind Wi-Fi device should be registered with authorities and ensure that no other mobile clients other than registered one is allowed in Wi-Fi network access for strengthening the security of Wi-Fi networks. University has rights to do lawful monitoring/logging of all internet user's activity and share it with statutory bodies, if warranted.

Any device that accesses Wi-Fi network shall:

- Protect the user account from unauthorized use by not sharing the credentials to others for any reasons/mean. User will be held responsible for any misuse of account. Maximum Number of

Concurrent (simultaneous) logins for a user account should be ONE device either laptop/tablet/mobile.

- Use the Internet Judiciously and adhere to other university/hostel policies.
- Incidences of actual or suspected non-compliance of this policy should be reported to University immediately.

Enforcement and Sanctions

The University reserves the right to disable user wireless network access because of any of the following reasons if found:

- Allowing other individuals (e.g. friends, co-workers, multiple devices etc.) to use account.
- Attempt to tamper/hacking the servers/network or overloading IT resources and assets by excessive bandwidth usage or using miss-configured devices or knowingly using a false identity.
- Download/Use/Store or transmit illegal copies of copyrighted materials or patented software/movies/songs etc. is violation of the regulatory laws that involve protection of data or privacy.

C. Disciplined Use

- Obey Indian Cyber Crime & State laws holistically;
- Respect other users' use of IT resources;
- Run up-to-date antivirus software; and
- Apply the latest security patches to all your software and devices.

D. Prohibited Use

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 illegal;

- **Illegal Activities –**
  - Using the University networks and Internet services for any illegal activity or that violates other Board policies, procedures and/or University rules;
  - No one is allowed to start private websites, take part in business related online activities or post advertisements;
  - The disseminating of computer viruses, the installation of cookies or other data collection devices or devices that can be used by hackers, or software that can attack the computer system;
  - Attempting to access restricted areas, or doing anything that restricts other people's ability to use the internet;

- It is strictly prohibited to use the internet to interfere with, or disturb other users, software designed to do that, reroute information or break into other people's accounts;

- Hacking other people's main systems or databases, carrying out piracy, tampering with other people's information and or disseminating private information;

- All the information that can be retrieved from the internet, which belongs to other people or organizations, unless clearly marked as "public" or unless you have the written permission of the owner, must not be downloaded or transferred in any way;

- **The installation and use of software: Any software installed on the campus's internet nodes should be legally obtained;**

- **Illegally obtained software should not be installed stored or used within CU's network and internet system.**

- **Violating Copyrights –**
  Copying/downloading/distributing copyrighted material without the owner's permission.

- **Plagiarism –**
  Representing as one's own work any material obtained on the Internet (such as research papers, term papers, articles, etc). When Internet sources are used in student work, the author, publisher and Web site must be identified.

- **Copying Software/Media Files –**
  Copying or downloading software without the express authorization of the system administrator; illegally downloading music, photos, movies or other such files.

- **DOWNLOADING MUSIC AND VIDEO – PEER- TO –PEER FILE SHARING**
  Copyrighted material, including most music, is often downloaded or distributed illegally using peer-to-peer file sharing software or "P2P," which allow computers to share files directly with other computers. There are countless P2P systems that allow you to download music and video files apparently for free. P2P have many serious problems:

  - Downloaded music and video files are usually copyrighted. After you retrieve a file using P2P, your computer becomes a server, offering the file to other P2P users and making you responsible for illegal distribution. Copyright holders are not required to warn you before taking legal action. Copyright violation can also result in criminal prosecution.
  - Once your computer is an illegal P2P server it can:
    - run more slowly
    - slow down the entire University network
    - result in a fine per song you share
  - Downloaded files can infect your computer with viruses, expose confidential information and lead to identify theft.
  - Using P2P can result in University disciplinary action, including termination, for misuse of University property.

- **Non-University Related Uses –**
  University networks and Internet services should not be used for non-University related purposes such as private financial gain, commercial, advertising or solicitation purposes.

- **Misuse of Passwords/Unauthorized Access –**
  Do not use other users' accounts and do not try to gain unauthorized access to data or resources.

- **Malicious Use/Vandalism –**
  Any malicious use, disruption or harm to the University networks and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

E. No Expectation of Privacy

The University retains control, custody, and supervision of all computers, networks and Internet services owned or leased by the University. The University reserves the right to monitor all computer and Internet activity by staff/students. Staff/Students have no expectation of privacy in their use of University computers, including email and stored files. Each person will respect the rights of others to the protection of the files they store on a computer and will not alter or damage such files.

F. Compensation for Losses, Costs and/or Damages

The student and/or the student's parent/guardian shall be responsible for compensating the University for any losses, costs or damages incurred by the University related to the violations of the University Internet Use Policy 2015-2016 and/or these rules, including investigation of violations.

G. University Assumes No Responsibility for Unauthorized Charges, Costs, or Illegal Use

The University assumes no responsibility for any unauthorized charges made by staff/students, including but not limited to credit cards charges, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

H. Validity

All usernames and password to access University network and internet services will be valid for one academic year (only for students); and All users will be allowed to log-in on only one device at a particular point of time.

Violation of this policy and guidelines is a serious offense and University shall have the rights to permanently seize the laptop/devices and/or initiate strong disciplinary action including termination from the University, if need arises based on the severity of non-compliance.

System Analyst
(Convener, Internet Committee)

Date: 02/12/2015