



## **INFORMATION TECHNOLOGY (IT) POLICY**

**NETAJI SUBHAS OPEN UNIVERSITY**  
**([www.wbnsou.ac.in](http://www.wbnsou.ac.in))**

**NKN Campus NETWORK**

**April 2019**

## CONTENTS

Preamble

Why IT Policy?

IT policies will be applicable

Summary of IT facilities available through NSOU network

Users of IT infrastructure

General Guidelines

Ethical Issues

Use of licensed software

Use of anti-virus & protection of software

E-Waste Management Policy



## **Preamble**

University has been provided 1Gbps internet connectivity through National Knowledge Network (NKN) for its Regional Campus at Kalayni, Nadia. Distribution of the bandwidth across the campus-LAN & Wifi is a very important aspect of network management. The bandwidth management should give priority to academic contents, research projects, University Website & E-mail facility etc. over general internet browsing and other utilities. Unless required for a specified purpose, any other broadband or internet connectivity installed by the Schools of Studies/ Departments other than the Campus-network should comply with the IT Policy.

## **Why IT Policy?**

The academic institutional networks are vulnerable to cyber attacks world wide and specifically in India owing to the idea of academic freedom and autonomy on the campus. With the enactment of Information Technology Act, 2000 and Information Technology Amendment Act, 2008 in India and ever increasing incidents of cyber crimes, it is necessary for all organizations and institutions, public or private; to define its own IT Policy and to enforce minimum information and network security standards across all departments.

Effective policies are a sign of due diligence and are often necessary in the event of an IT audit or litigation. Policies also serve as blueprints that help the institution for implementing IT security measures.

In the Regional Campus of NSOU at Kalyani, it has become essential to enact a useful IT policy and guidelines for the following reasons:

- To ensure smooth operations of IT infrastructure and access to internet
- To protect its vital information like examination results data, accounts data etc. from unauthorized access
- To make available minimum internet bandwidth to each academic user to ensure the availability of academic e-resources
- To enforce and ensure minimum information & network security standards to prevent any misuse from its own users and outsiders
- To protect its IT infrastructure from cyber attacks and to prevent it from being used as a platform to create a cyber attack somewhere outside the campus
- To Control on activities on the university network that are not related to academic and administrative of the university.

## **IT policies will be applicable**

Hardware & Software Installation  
Use of Network (Intranet & Internet)  
Use of E-mail Account  
Hosting of Web Site  
Use of university Database

## **Summary of IT facilities available through NSOU network**

- Access to the Information Highway of Internet using 1Gbps of Internet bandwidth
- Official Web Site ([www.wbnsou.ac.in](http://www.wbnsou.ac.in))

- Mail accounts with NSOU domain name ([x@wbnsou.ac.in](mailto:x@wbnsou.ac.in)) for faculty and administrators
- Access to the online Journals subscribed by NSOU
- Access to the NSOU online Library services
- Troubleshooting support in resolving network related problem
- Web conferencing with other institutions anywhere in the World
- OER Repository

### **Users of IT infrastructure**

A 'User' means any person, who is authorized to have access to IT infrastructure of the university. It includes faculty members, Officers, administrative staff, enrolled students and guests i.e. registered participants of workshop/ conference etc.

### **General Guidelines**

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. The campus-LAN and Wifi are meant for official use arising from the academic/research activities and administrative responsibilities of the faculty, staff and students of the University. Use of IT and network resources for personal purposes is prohibited.
3. Users should view the IT & network resources with a sense of ownership and participation, and should actively help to prevent any misuse.
4. The IT Cell under the competent authority 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. The IT Cell is authorized to 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.
5. IT Policy Committee (IT-PC) shall look into all violations of this policy, and recommend suitable action to the University Authorities.
6. All the users of the university campus network will automatically agree to abide by the provision of this policy. All individuals who use IT & network resources of the university should be made aware of this policy through NSOU website.
7. The user department may update information of its users once in a year. The modification of user data for teaching/non-teaching staff and any other user must be updated immediately by the user department with the change in the user status. Individual user is not responsible for updating of his/her information in the user database.
8. Access of non-academic websites, download of music/movies and non-academic videos etc. must be restricted for all users.

9. IT Cell will decide which web sites can be accessed through the campus internet and, shall disallow access to other sites and maintain a mechanism suitable to enforce such a purpose under the guidance and supervision of IT Policy Committee.
10. Users of a user department can access the network via desktop/laptop computers on the campus network. Users are responsible and accountable for the usage of the systems allocated to them.
11. Users must take adequate & appropriate measures to prevent misuse of network from computer systems that they are responsible for.
12. 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.

### **Ethical Issues**

1. The Intranet and Internet access will not be used for commercial activity, personal advertisement, solicitations, or promotions, such as hosting or providing links of commercial websites or email broadcasts of commercial promotions to the users.
2. Any part/component of the IT infrastructure of the university shall not be misused for Anti-University, Anti-State or Anti-Government activities.
3. The IT Policy Committee will be authorized to undertake appropriate measures to ensure maintenance of such discipline and initiate suitable actions for prevention of misuse of university IT and network resources.
4. 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.
5. No user other than those registered with the University, can be used to connect to the intranet/ internet.
6. The downloading of audio and video files is to be done strictly for academic/official purposes.
7. Each user must preserve & maintain the confidentiality of the password used by him/her. No user must try to access the IT resources using other user's password, either knowingly or otherwise.
8. 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.



9. Use of network Office equipment like Network Printers and Network Scanners should be encouraged.
10. Backup of confidential official data on personal laptops, external hard drives or any other mobile / removable media should be discouraged.
11. No user/user department should take official data outside the NSOU campus without authorization.
12. No person shall publish post or release any information that is considered confidential or not for public.
13. No person shall use logo or intellectual property content/ materials on their personal page or social media.
14. No person shall disparage the university, present or past employees, learners and faculties etc.

#### **Use of licensed software**

1. 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.
2. Use and exchange of pirated / illegal software over the NSOU-Intranet is prohibited. It is the responsibility of the head of the user department to ensure compliance.
3. The downloading and use of software that is not characterized as public domain or 'free' is prohibited.
4. Use of Open Source Software is encouraged to avoid the financial burden and legal complications arising out of license management.

#### **Use of anti-virus & protection of software**

1. The user department is responsible for the installation and maintenance of proper Anti-virus or Internet/Endpoint Security/Protection Software or any other security software as prescribed.
2. In case of detection of any issues in the security, the compromised computer/ equipment must be disconnected from the NSOU-Intranet failing which IT Cell shall disable the respective network connection.
3. Strict action may be taken by the IT Policy Committee against users who deliberately prevent the installation of such security software or disable such software or prevent them from running.

#### **E-Waste Management**

##### **a) Introduction**

E-waste is a general category for electronic products facing displacement or replacement

that are hazardous due to the toxic metals present with their internal materials, coatings and glass. E-waste contains metals and other materials that can be hazardous to human health and the environment if they are not properly managed. Netaji Subhas Open University acknowledges the need for proper e-waste handling and disposal.

**E-waste Definition:** Electronic waste or e-waste may include personal computers, monitors, televisions, keyboards, printers, telephones, typewriters, calculators, copiers, fax machines and audio equipment.

**E-waste Policy Guidelines:**

- a) Netaji Subhas Open University endeavors to ensure environmental conservation and protection from the effects of e-waste.
- b) Netaji Subhas Open University recognizes:
  - i) The need to dispose e-waste in manner that is safe and sound with respect to its staff, students, and Institutional operations.
  - ii) The need to establish clear guidelines on e-waste management.

The university is having a provision to constitute an e-waste advisory committee to implement above mentioned policy under the chairmanship of Vice Chancellor or Chairman, nominated by Vice Chancellor.

**University has the following members in the advisory committee.**

Chairman: Vice Chancellor/ his Nominee

- Members:
- i) Registrar
  - ii) Finance officer
  - iii) Director CIQA
  - iv) Administrative Heads of Regional Centres
  - v) Technical Member Related to ICT (Nominated by VC)

**b) Implementation**

1. All Netaji Subhas Open University surplus electronic devices, including computers and computer peripherals, must be sent to the Director, Computer Centre/E- Waste Management team to determine if the surplus electronic device should be donated to local schools as specified by the advisory committee, or should be sold through as per policy of Netaji Subhas Open University, or should be recycled.
2. The Registrar/Finance Officer/ Head of Regional Centres, Netaji Subhas Open

University will be responsible for inventory control of surplus electronic devices and relaying asset numbers to the Central Receiving Inventory Supervisor to remove items from university inventory as per recommendation of advisory committee.

3. E-Waste Management team will pick up e-waste items from the Departmentor section based on recommendation of Administrative Heads of the Headquarters/Regional Centres and his team. Items must be categorized for recycling purpose or donation purpose as per recommendation of advisory committee.
4. The Registrar/ Finance Officer/ Stores In-Charge, Netaji Subhas Open University is responsible for record keeping and certification of disposal for all e-waste as per recommendation of advisory committee.

c) Responsibilities

Registrar/Finance Officer/ Stores in-charge Netaji Subhas Open University, or Director/Deputy Director(RC) or E-Waste management team is responsible for adhering to this policy and will ensure that their subordinates adhere to this policy. Any employees of E-waste management team who fail to comply with this policy may be subject to disciplinary action for noncompliance with university policies.

d) Review Policy

The policy shall be reviewed after every five years or earlier, as need arises.

***Developed by the IT Policy Committee.***

***Members:***

1. Professor Sanjit Kumar Setua, Department of Computer Science, University of Calcutta
2. Dr. Debojyoti Konar, Registrar, Presidency University
3. Professor Anirban Ghosh, Director, School of Professional Studies & School of Vocational Studies, Director (Addl. Charge), Regional Centre, Kalyani, Netaji Subhas Open University
4. Mr. Hillol Ghosh, Informational Technology Officer, Netaji Subhas Open University