NETAJI SUBHAS UNIVERSITY

Estd. Under Jharkhand State Private University Act, 2018

IT POLICY

Registrar
Netaji Subhas University
Jamshedpur, Jharkhand

VICE CHANCELLOR
NETAJI SUBHAS UNIVERSITY
JAMSHEDPUR, JHARKHAND

Table of Contents

1. Abbreviation

Sl. No.	Abbreviation	Description
1.	NSU	Netaji Subhas University
2.	CA	Competent Authority
3.	IA	Implementing Agency
4.	LAN	Local Area Network
5.	GoI	Government of India
6.	IT	Information Technology
7.	ICT	Information and Communication Technology
8.	IP	Internet Protocol
9.	DHCP	Dynamic Host Configuration Protocol
10.	IR	Institutional Repository
11.	EULA	End User License Agreement
12.	CAPEX	Capital Expenditure
13.	OPEX	Operational Expenditure

2. Introduction

At Netaji Subhas University (NSU), we provide a range of IT resources to support the educational, research, administrative, and instructional activities of the university. These tools are designed to help students, faculty, staff, and other members of the NSU community access and manage the information necessary for their work. By utilizing these resources, users can stay informed and complete their tasks more efficiently and effectively.

This document outlines the specific guidelines for using all IT resources at NSU. The policy applies to everyone who uses the university's computing resources, including (but not limited to) faculty, visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, affiliated colleges, and any other entity that accesses NSU's network services.

For clarity, the term "IT Resources" refers to all hardware and software that is owned, licensed, or managed by the university, as well as any access to the university network, whether through a physical or wireless connection—regardless of whether the device used is owned by the individual or the university.

It is important to understand that misuse of these resources can pose risks and liabilities for the university. Therefore, these IT resources are meant to be used primarily for university-related activities and should always be used in a lawful and ethical manner.

3. Scope

This policy outlines the guidelines for using IT resources from the perspective of the end user. It applies to everyone, including individuals, users, and entities, as described in Section 2, who access and use NSU's IT resources.

4. Objective

The goal of this policy is to ensure that NSU's IT resources are used properly and to prevent any misuse by users. By using the resources provided by NSU, users agree to follow this policy.

- The university's IT policy is in place to maintain, protect, and ensure the legal and proper use of the technology infrastructure on campus.
- This policy sets university-wide guidelines and outlines the responsibilities for safeguarding the confidentiality, integrity, and availability of the university's information assets.
- The information assets covered by this policy include data, information systems, computers, network devices, intellectual property, and both documents and verbally shared information.

5. Roles and Responsibilities

The following outlines the roles and responsibilities expected of each party involved:

- **NSU** will implement the necessary controls to ensure users comply with this policy. The Computer Centre will be the primary body responsible for implementing and providing support in this regard.
- **The Computer Centre** will handle and resolve any incidents related to the security of this policy, providing the necessary support as needed.
- Users must use NSU's IT resources for activities that align with the university's academic, research, and public service mission, and avoid engaging in any "Prohibited Activities."
- All users are required to comply with relevant national, state, and local laws.
- Users must adhere to existing telecommunications and networking laws and regulations.
- Users must follow copyright laws, particularly when dealing with protected commercial software or intellectual property.
- As part of the NSU community, users are provided with access to scholarly and work-related tools, such as the library, specific computer systems, software, databases, and the internet. It is expected that users will have a reasonable expectation of unobstructed use of these tools, privacy, and protection from misuse by others sharing these resources. Users can expect their rights to access information and express opinions to be protected, just as they would be for paper and other non-electronic forms of communication.
- Users are prohibited from installing any network or security devices on the NSU network without consulting the implementing agency first.
- It is the responsibility of all members of the university community to familiarize themselves with the regulations and policies related to the appropriate use of NSU's technology and resources. Users must exercise good judgment in the use of these resources. Just because something is technically possible does not mean it is appropriate.
- As representatives of the NSU community, all individuals are expected to uphold the university's reputation in all activities related to the use of ICT communications, both within and outside the university.
- The **Competent Authority** at NSU is responsible for ensuring that this policy is properly communicated across the university.

6. Acceptable Use

- **Authorized users** are only allowed to use the IT resources they've been granted access to. No user should use another person's account or try to guess or captured someone else's password.

- Users are individually responsible for the proper use of any resources assigned to them, including computers, network addresses or ports, software, and hardware. As an authorized user, you are accountable to the university for how these

resources are used. You should not allow unauthorized individuals to access the network by using NSU's IT resources or any personal device connected to NSU's campus-wide Local Area Network (LAN).

- The university is bound by its End User License Agreement (EULA), which covers certain third-party resources. Users are expected to comply with these agreements when accessing such resources.

- Users should take reasonable steps to protect the passwords and ensure that resources are secured against unauthorized access or use.

- No user should attempt to access restricted areas of the network, operating systems, security software, or any other administrative applications without proper authorization from the system owner or administrator.

- Users must follow any specific policies or guidelines for the resources to which they've been granted access.

- If other policies are more restrictive than this one, the more restrictive policy will take precedence.

7. Privacy and Personal Rights

- All users of the university's IT resources are expected to respect the privacy and personal rights of others.

- Do not access, copy, or tamper with another user's email, data, programs, or files without proper authorization and approval from the Competent Authority (CA).

- While the university typically does not monitor or restrict the content of information transmitted over the campus-wide LAN, it does reserve the right to access and review such information under specific conditions, with prior approval from the Competent Authority.

8. Privacy in Email

While NSU makes every effort to protect the privacy of email users, complete privacy cannot always be guaranteed. Since employees are provided with electronic systems and network services to conduct university business, there may be situations where, with approval from the competent authority, the university reserves the right to access and review stored information, but only with the users consent.

User Compliance

By using NSU's IT resources and accepting any university-issued computing accounts, an individual agrees to follow this policy as well as all other related computing policies. It is the individual's responsibility to stay informed about any updates or changes to NSU's IT policies and adjust accordingly when needed.

9. Access to the Network

9.1. Access to Internet and Intranet

- Before connecting a client system to the university's campus-wide LAN, users must register the system and obtain one-time approval from the competent authority.
- NSU maintains two separate networks: the Internet and the Intranet. These networks are kept entirely separate with no physical connection or devices linking them. Endpoint compliance will be enforced on both networks to prevent unauthorized access to data.
- Users should not attempt to bypass network filtering or engage in any activities through websites or applications that could compromise the network's performance or security.

9.2. Access to NSU's Wireless Networks

To connect to NSU's wireless network, users must follow these guidelines:

- Users must register the IR access device and obtain one-time approval from the competent authority before connecting it to NSU's wireless network.
- Wireless client systems and devices will not be allowed to connect to NSU's wireless access points without proper authentication.
- For security reasons, users are advised not to connect the IR devices to unsecured wireless networks.

9.3. Filtering and blocking of sites:

- The Computer Centre or any other Implementing Agency (IA) may block internet content that violates the IT Act 2000 or other relevant laws, or content that could pose a security risk to the network.
- The Computer Centre or any other Implementing Agency (IA) may also block content that, in the university's opinion, is inappropriate or could negatively impact the productivity of users.

10. Monitoring and Privacy

- The Computer Centre or any other Implementing Agency (IA) has the right to regularly audit networks and systems to ensure compliance with this policy.
- For security reasons or to comply with applicable laws, the IA/Nodal Agency may access, review, copy, or delete any electronic communications or files stored on university-provided devices, with prior notification to the user. This includes files, emails, posts on electronic media, internet history, and more.
- The IA may monitor users' online activities on the university network, in accordance with the Standard Operating Procedures and norms set by the Government of India.

11. E-mail Access from the University Network

- The email service authorized by NSU and managed by the Computer Centre should be used exclusively for official correspondence.

- For more information, please refer to the "E-mail Usage Policy of NSU.

12. Access to Social Media Sites from NSU Network

- The use of social networking sites by NSU users is governed by the "Framework and Guidelines for the Use of Social Media for Government Organizations.

- Users must comply with all provisions under the IT Act 2000 when posting any information on social media.

- Users are required to follow the "Terms of Use" of the relevant social media platform and adhere to laws related to copyright, privacy, defamation, contempt of coIRt, discrimination, harassment, and other applicable regulations.

- Users should report any suspicious incidents to the competent authority as soon as possible.

- Users are encouraged to use high-security settings on their social media accounts to protect their privacy.

- Users must not post any content that is offensive, threatening, and obscene, infringes on copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or otherwise unlawful.

- Users must not disclose or use any confidential information obtained in their role as an employee of the university.

- Users should avoid posting any content or making comments that could damage NSU's reputation.

13. Use of IT Devices Issued by NSU

IT devices issued by NSU to users are intended primarily for academic, research, and other university-related activities, and should be used in a lawful and ethical manner. These devices must also follow the guidelines outlined in the section "Use of IT Devices on NSU Network." This section includes best practices for using desktop devices, portable devices, external storage media, and peripheral devices like printers and scanners.

Security Incident Management Process

- A security incident refers to any event that negatively affects the availability, integrity, confidentiality, or authority of the university's data.

- The Implementing Agency (IA) has the right to deactivate or remove any device from the network if it is considered a threat and could compromise a system. The

competent authority of the university will be informed in such cases.

- Any security incident should be reported immediately to the Indian Computer Emergency Response Team (ICERT) and the IA.

- Despite the previous clauses, if necessary, the IA may disclose logs related to any IT resources to law enforcement agencies or other organizations, in accordance with the IT Act 2000 and other applicable laws.

- The IA will not accept or act on any requests from other organizations to review or release logs, except as specified in this policy.

14. Intellectual Property

The material available through NSU's network and resources may be protected by privacy, publicity, or other personal rights, as well as intellectual property rights, including copyrights, patents, trademarks, trade secrets, or other proprietary information. Users must not use NSU's network and resources in any way that could infringe upon, dilute, misappropriate, or violate these rights.

Enforcement

- This policy applies to all users of NSU, as outlined in Section 2 of this document. It is mandatory for everyone to follow the rules and guidelines set forth in this policy.
- Each department or unit within NSU is responsible for ensuring compliance with this policy. The Implementing Agency will provide the necessary technical support to help user entities meet these requirements.

15. Deactivation

- If there is any security threat to NSU's systems or network caused by the resources a user is using, the Implementing Agency (IA) may immediately deactivate those resources.

- After deactivation, the concerned user and the university's competent authority will be notified.

16. Audit of NSU Network Infrastructure

The security audit of NSU network infrastructure shall be conducted periodically by an organization approved by the university.

17. Review

Any future changes to this policy, as needed, will be made by the Technical Committee (ICT) with the approval of the university's Competent Authority.

18. IT Hardware Installation Policy

The university network user community needs to take certain precautions when installing their computers or peripherals to minimize the inconvenience caused by service interruptions due to hardware failures.

(i) Who is a Primary User?

A "primary" user is an individual in whose room the computer is installed and primarily used. If multiple users share a computer, but none are considered the "primary" user, the department head should designate someone to take responsibility for compliance.

(II)What are End-User Computer Systems?

In addition to client PCs, servers not directly managed by the Computer Centre are also considered end-user computers. If no primary user can be identified for these systems, the department will assume responsibility for them. Computer systems that act as servers, providing services to other users on the Intranet/Internet, are still treated as "end-user" computers under this policy, even if registered with the Computer Centre.

(III)Warranty & Annual Maintenance Contract

Computers purchased by any section, department, or project should ideally come with a 3-year onsite comprehensive warranty. After the warranty expires, the computers should be covered by an annual maintenance contract, which includes standard repair and maintenance procedures as defined by the Computer Centre.

(IV)Power Connection to Computers and Peripherals

All computers and peripherals must be connected to a power supply through a UPS (Uninterruptible Power Supply). The UPS should never be turned off, as it needs continuous power to recharge its battery, except when the UPS is left unattended. Additionally, the UPS systems should be connected to electrical points that are properly earthed and have correctly installed wiring.

(V)Network Connection

When connecting a computer to the network, the network cable should be kept away from any electrical or electronic equipment, as these can interfere with network communication. Also, ensure that no other electrical or electronic equipment shares the same power supply as the computer and its peripherals.

(VI)File and Print Sharing Facilities

File and print sharing should only be enabled on the computer over the network when absolutely necessary. When sharing files, they should be protected with a password and set to "read-only" access to ensure security.

(VII)Maintenance of Computer Systems Provided by the University

For all computers purchased centrally by the university and distributed by the Estate Branch, the University Computer Maintenance Cell, attached to the Computer Centre, will handle any maintenance issues and respond to related complaints.

19. Software Installation and Licensing Policy

Any computers purchased by individual departments or projects must ensure that all necessary licensed software (including the operating system, antivirus software, and required application software) is installed.

In line with anti-piracy laws, the university's IT policy strictly prohibits the installation of pirated or unauthorized software on university-owned computers or those connected to the campus network. If any such unauthorized software is found, the university will hold the department or individual responsible for its presence on the computers in their respective areas.

A. Operating System and its Updating

Individual users should make sIRe that respective computer systems have theirs updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or so.

University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

B. Use of software on Desktop systems

Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority. Any software installed should be for activities of the university only.

C. Antivirus Software and its updating

All computer systems used at the university must have antivirus software installed and running at all times. The primary user of each computer is responsible for ensuring that the system complies with this virus protection policy.

Users should regularly check that the IR computers have up-to-date antivirus software installed and properly maintained.

D. Backups of Data

Individual users should perform regular backups of the IR vital data. Users should keep the IR valuable data backups in external storage devices such as pen drives, external HDD etc.

20. Use of IT Devices on NSU Network

This section outlines the best practices for using desktop devices, portable devices, external storage media, and peripheral devices like printers and scanners on NSU's network.

a. Desktop Devices

1) Use and Ownership

Desktops should primarily be used for university-related work. If personal use is necessary, users should exercise good judgment and keep it to a minimum.

2) Security and Proprietary Information

Users must get prior approval from the Implementing Agency (IA) before connecting any device to NSU's network.

b. Users should keep the IR passwords secure and never share the IR account details. Passwords should be strong and comply with the application's password policy.

c. All active desktop computers must be secured with a password-protected screensaver, which should automatically activate after 10 minutes or less of inactivity, or the system should be logged off when unattended.

d. Users must ensure that virus-scanning software is up-to-date on all systems and be cautious when opening email attachments from unknown senders, as they may contain viruses, email bombs, or Trojan horse code.

e. Any loss of data or accessories should be reported to the IA and the university's competent authority.

f. Users need prior authorization from the competent authority before taking any NSU-issued desktop off-campus.

g. Users must shut down the IR systems properly before leaving the office or department.

h. Users should follow any instructions or procedures provided by the Computer Centre.

i. If a user suspects that the IR computer has been infected with a virus (e.g., it's

behaving erratically or running slowly), they should report it to the IA (Computer Centre) for further action.

b. Sharing of data

Users should never share the IR account information, passwords, Personal Identification Numbers (PINs), digital signature certificates, or any other information or devices used for identification and authorization purposes.

c. Use of Portable devices

This section applies to devices provided by NSU, such as laptops, mobiles, iPads, tablets, PDAs, and others. The use of these devices should follow the guidelines below:

- **Device Responsibility**: If someone else uses your NSU-issued device without authorization, you'll be responsible for any issues that arise from that usage.
- **Keep Devices Secure**: Always keep your NSU-issued device with you or store it in a secure location when not in use. Avoid leaving it unattended in public places like classrooms, meeting rooms, or restaurants.
- **Password Protection**: Make sure your device is password-protected and set to automatically lock when not in use. The password should be as strong as possible and follow the application's password policy.
- **Device Maintenance**: The Computer Centre will ensure that all devices have the latest operating system, antivirus software, and application updates, in coordination with you. Firewalls should be turned on where applicable.
- **Deleting Data**: Before returning or disposing of a device, make sure to securely delete all personal data.
- **Report Lost or Stolen Devices**: If your device is lost, stolen, or misplaced, report it immediately to the IT department and the relevant authority.
- **Installing Software**: Before installing any software, review the app's permissions to ensure your personal information is not being shared without your consent.

21. Network (Intranet & Internet) Use Policy

The University provides network connectivity, referred to as "the Network," either through an authenticated network connection or a Virtual Private Network (VPN). This network use is governed by the University's IT Policy. The Computer Centre is responsible for maintaining and supporting the Network, but local applications are not included. If you encounter any issues with the University's network, please report them to the Computer Centre.

A. IP Address Allocation

Any device (PC or Server) that connects to the University network must have an IP address assigned by the Computer Centre. IP addresses will be allocated based on a Virtual LAN (VLAN) that's set up for each department or purpose. Devices can only be assigned IP addresses from the IR specific VLAN address pool. Additionally, each network port in the room where the device is connected will be bound to a specific IP address to prevent unauthorized use from other locations.

Whenever a new device is set up, it will be assigned an IP address according to the DHCP pool policies.

A. DHCP and Proxy Configuration by Individual Departments /Sections/ Users

- Using any computer at an end-user location as a DHCP server to connect more devices through a personal switch or hub, and distributing IP addresses (whether public or private), is strictly prohibited. This is a violation of the University's IP address allocation policy. Similarly, setting up proxy servers is not allowed, as it can interfere with services managed by the Computer Centre.
- Even connecting another computer to a device that has been configured with an additional network interface card is considered a proxy/DHCP setup.
- If the IP address allocation policy is not followed, the port to which the device is connected will be disconnected. The connection will only be restored once the relevant department or user provides written assurances that they will comply with the policy.

B. Running Network Services on the Servers

a. If a department or individual wants to run server software (like an HTTP/Web server, SMTP server, or FTP server) on the University network, they must inform the Computer Centre in writing. They also need to meet the requirements outlined in the University's IT policy for running such services. Failing to do so is a violation of the IT policy, and the network connection will be terminated.
b. The Computer Centre is not responsible for the content on any machines connected to the University network, whether they are University-owned or personal devices.
c. If any machine connected to the network is found to have potentially harmful software, the Computer Centre will disconnect it from the network. A machine may also be disconnected if its activities negatively affect the performance of the network.
d. When accessing remote networks through the University's network connection, you must follow the policies and rules of those external networks. This applies to all networks the University is connected to. Additionally,

University network resources cannot be used for personal commercial activities.

e. For security and performance reasons, network traffic will be monitored by the Computer Centre.
f. Impersonating an authorized user when connecting to the network is a serious violation of this policy and will result in the termination of the connection.

C. Internet Bandwidth obtained by Other Departments

- Any internet bandwidth acquired by a department for a research program or project should ideally be combined with the university's general internet bandwidth and treated as a shared resources for the university.
- If, for any reason, pooling the bandwidth with the university's network isn't possible, that network should be completely separated from the university's campus network. All computers connected to that network should have the IR own separate VLANs based on appropriate groupings.
- The IP address scheme (whether private or public) and the university's gateway should not be used as an alternative gateway. Networks like this should be properly secured with the necessary network security measures as outlined in the university's IT policy. A network diagram, including details about the design and IP address schemes, should be submitted to the Computer Centre.
- Failing to comply with this policy is considered a direct violation of the university's IT security policy.

22. Email Account Usage Policy

NSU offers official email access to all its users. To streamline communication across the university—between the administration, faculty, staff, and students—it is highly recommended that you use the official email provided by Netaji Subhas University.

Using the university's email service for formal communications ensures efficient delivery of important messages to everyone, including faculty, staff, students, and university administrators. These communications may include administrative updates, policy messages, official announcements, and more.

To receive these critical updates, it's important to keep your university email active by using it regularly. Faculty and staff can access the IR email by logging into Gmail with the IR User ID and password. If you don't have a university email account yet, you can request one by contacting the Computer Centre and submitting an application in the prescribed form.

By using the university's email system, you agree to follow these guidelines:

1. **Official Use**: The email facility is primarily for academic and official purposes, with limited use for personal communication.

2. **No Illegal/Commercial Use**: Using your email for illegal or commercial activities is a direct violation of the university's IT policy. This includes, but is not limited to, unauthorized distribution of software, sending unsolicited bulk emails, and creating harmful or fraudulent messages or images.
3. **Attachments**: When sending large attachments, ensure that the recipient can handle them. Some email systems may not accept large files.
4. **Mailbox Space**: Keep your mailbox usage under about 80%. If your mailbox is full, incoming emails, especially those with large attachments, may bounce back.
5. **Security**: Don't open emails or attachments from unknown or suspicious soIRces. Even if the email seems to be from someone you know, be cautious if there's an attachment or if the message seems strange. Confirms with the sender if necessary to avoid viruses or other security threats.
6. **Protect Your Credentials**: Never share your email account credentials with others. You are personally responsible if your account is misused.
7. **Privacy**: Do not attempt to access or intercept someone else's email account. Doing so invades the IR privacy and violates the policy.
8. **Shared Computers**: If you're using a shared computer and another user has left the IR email account open, make sure to close it before using the computer. Avoid viewing any of the email contents.
9. **Impersonation**: Impersonating someone else's email account is a serious violation under the IT security policy and will be treated as an offense.
10. **Your Responsibility**: It's your responsibility to ensure your email account follows the university's email usage policy.
11. **Spam Folder**: Emails flagged as spam will go into your SPAM_MAIL folder. Please check this folder regularly for any important emails that may have been mistakenly marked as spam. It's also a good idea to empty your spam folder frequently.

These guidelines (1 to 11) also apply to personal email services such as Gmail, Yahoo, Hotmail, RediffMail etc., when used on the university campus network or with university resources, even if accessed from outside the campus.

23. Institutional Repository (IR)

Netaji Subhas University shall be providing services related to Institutional Repository (IR) through Central Library of the university as per the following policies

23.1. What is an Institutional Repository (IR)?

An Institutional Repository (IR) is a service offered by the University Library that helps manage and share digital materials created by the University and its community members. Essentially, it's the University's way of ensuring that these materials are preserved for the long term and are easily accessible to its users.

23.2. What Does the IR Contain?

The IR contains a variety of digital documents, based on the University's policies. Common items include research outputs like journals articles (pre-prints and post-prints), conference

papers, technical reports, software, technical manuals, audio and video recordings, e-books, seminar/webinar lectures, theses, dissertations, rare books, and more. It also includes grey literature (non-traditional documents), such as convocation addresses, student handbooks, and teaching materials.

While Netaji Subhas University's IR will focus mainly on research and academic publications, it may eventually integrate with the University's courses management system and include e-learning features.

23.3. Who Can Access the NSU IR?

The IR is accessible primarily to members of the University community, including faculty, research scholars, students, and staff who have an official university email address (@nsuniv.ac.in).

23.4. How to Access the IR?

Registered members can browse the NSU IR and download materials in PDF format for academic purposes, using the IR institutional email address. Access is subject to providing general information through the University's Central Library.

23.5. How Long Can You Access the IR?

Faculty, researchers, and students can access the IR as long as they are part of the University. Once the IR tenure or course ends and they've received a no-dues certificate from the University Library, the IR access to the IR will be revoked.

23.6. Copyright and IR Use

The materials in the NSU IR are often grey literature, and downloading these materials comes with copyright restrictions. These materials cannot be reprinted or sold for commercial purposes. Any member found violating these copyright rules will be treated according to the provisions of the Copyright Act of 1957. Additionally, user IDs and passwords are personal and non-transferable. Sharing them or violating the University's SOPs will lead to penalties.

24. Disposal of ICT equipment

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the university. University has already a MOU regarding the same.

25. Budgetary provisions for ICT

At Netaji Subhas University (NSU), the use of ICT (Information and Communication Technology) facilities has always been encouraged, especially since the University is located in a remote area. This has allowed us to keep up with other universities and provide our students with modern resources. With this in mind, NSU plans to allocate budgetary provisions in the following ways:

- **Recurring Grants (OPEX)**: We will allocate funds under recurring grants to maintain the current ICT infrastructure and ensure that all ICT-enabled services continue to run smoothly.
- **Upgrades and Expansion (CAPEX)**: Adequate funds will be set aside for the upgrading and expansion of ICT infrastructure to meet the growing needs of the University.
- **New ICT Solutions**: We will also allocate capital funds for implementing new and innovative ICT solutions whenever needed.
- **Supporting Student Growth**: As student enrolment has increased by 10% each year, we believe it's essential to provide more support for ICT facilities. Therefore, 10% of the University's total budget will be dedicated specifically to improving ICT resources, especially for students.

26. Breach of This Policy

We encourage all users to stay alert and report any suspected violations of this policy to the IT Helpdesk at kkyadav@nsuniv.ac.in as soon as possible. Once the University is notified or becomes aware of any potential policy breach, we reserve the right to suspend a user's access to University data.

If a breach is confirmed, additional actions may be taken, including disciplinary measures such as dismissal for staff, expulsion for students, or termination of contracts for third parties, in line with the University's disciplinary procedures.

27. Revisions to Policy

The University has the right to update or revise this policy at any time. Any changes will be recorded in the policy's revision history, which can be found on the NSU website. By continuing to use the University's IT resources after any update, you are considered to have accepted the revised terms of the policy.

28. Contact Us

If you have any queries in relation to this policy, please contact:

Email: kkyadav@nsuniv.ac.in

Appendix – I: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Teachers & Staff only)

First Name	:	
Middle Name	:	
Last Name	:	
Department/ Branch	:	
Current Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department/ Controlling Officer.
4. An official Email address would be created within 24hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department/ Controlling Officer)

Appendix – II: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Research Scholars only)

First Name	:	
Middle Name	:	
Last Name	:	
Department	:	
Name of the PI	:	
Name of the Project	:	
Duration of Research	:	
Current Email address*	:	
Phone Number	:	
Admission Year*	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department and Principal Investigator.
4. An official Email address would be created within 24 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Principal Investigator)

Appendix – III: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

(For Students only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department	:	
Corse	:	
Semester	:	
Roll No.	:	
Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department.

(Signature of the Head of the Department)

Appendix – IV: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

(For Employees only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department/ Branch	:	
Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Controlling Officer.

(Signature of the Controlling Officer)