IT POLICY & GUIDELINES

February 2022, Version 1.0

নৰ্থ লখিমপুৰ কলেজ (স্বায়ত্তশাসিত)
North Lakhimpur College
(AN AUTONOMOUS COLLEGE AFFILIATED TO DIBRUGARH UNIVERSITY)

North Lakhimpur College (Autonomous)

Khelmati , North Lakhimpur pin-787031

Table of Contents

1. Abbreviation

Sl. No.	Abbreviation	Description
1.	NLC	North Lakhimpur College
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

2. Preamble

North Lakhimpur College (Autonomous) provides information technology resources to support the college's educational, instructional, research, and administrative activities, as well as to improve employee efficiency and productivity. These tools are intended to help them access and process information relevant to their fields of work. These resources assist them in staying informed and performing their duties efficiently and effectively.

This document establishes specific guidelines for the use of all NLC IT resources. This policy applies to all users of NLC-owned or managed computing resources. Individuals covered by the policy include (but are not limited to) NLC faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, and any other entity managed by NLC that accesses network services through NLC's computing facilities.

The term 'IT Resources' refers to all hardware and software owned, licensed, or managed by the college, as well as use of the college network via a physical or wireless connection, regardless of who owns the computer or device connected to the network. Misuse of these resources can expose the college to unnecessary risk and liability. As a result, it is expected that these resources will be used primarily for college-related purposes and in a lawful and ethical manner.

3. Applicability

The IT Policy applies to all College faculty, staff, and students, as well as anyone else who accesses, transmits, or stores various types of related information, whether personally or through College-owned IT resources..

4. Objective

Each user of the College Information Resources must ensure that they are used to advance the College's mission of teaching, learning, research, and administration, and that they are not mishandled by the users. The use of NLC resources implies that the user agrees to be bound by this policy. The following are the main goals of this document:

- The purpose of the NLC IT policy is to maintain, secure, and ensure the legal and appropriate use of the College's information technology infrastructure on campus.
- This policy establishes college-wide strategies and responsibilities for ensuring the Confidentiality, Integrity, and Availability of the information assets that the College accesses, creates, manages, and/or controls. Data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information are all covered by the policy.
- The policy ensure that all College users are held accountable for adhering to the procedures governing the implementation of this Policy document and any other matters incidental to those rules.

5. Roles and Responsibilities

1) NLC would then put in place appropriate controls to ensure that their users follow this policy. The Computer Centre will serve as the primary Implementing Agency and will provide all necessary assistance.
2) Computer Centre will ensure that all incidents involving the security aspects of this policy are resolved by their users. The Implementing Agency will provide the necessary assistance in this regard.
3) Use NLC's IT resources for activities that are consistent with the College's academic, research, and public service missions and are not "Prohibited Activities."
4) All users must follow current national, state, and other applicable laws. Follow current telecommunications and networking laws and regulations.
5) Follow copyright laws when dealing with commercial software or intellectual property that is threatened.
6) NLC provides scholarly and/or work-related tools to members of the NLC community, including access to the Library, certain computer systems and servers, software and databases, and the Internet. The College Community is expected to have a reasonable expectation of unrestricted access to these tools, certain levels of privacy, and protection from abuse and intrusion by others who share these resources. Authorized users can expect their right to access information and express themselves to be protected in the same way that it is for paper and other non-digital communication.
7) Users of the NLC must consult the IA (Implementing Agency) before installing any network/security device on the network.
8) It is the responsibility of the College Community to be aware of the College's regulations and policies regarding the proper use of the College's technologies and resources. The NLC Community is responsible for using the College's technological and information resources responsibly. Just because something is technically possible doesn't mean it's a good idea to carry it out.
9) Each individual is expected to respect and uphold the College's good name and reputation in any activities involving the use of ICT communications within and outside the college as a representative of the NLC community. The NLC's Competent Authority (CA) should ensure that this policy is properly disseminated.

6. Appropriate Use

- An authorized user can only use the IT resources for which he or she has been granted access. No one should use another person's account or try to guess or capture other people's passwords.
- All resources assigned to a user, including the computer, the network address or port, software, and hardware, are used appropriately by the user. As a result, he or she is responsible to the College for all resources used. As an authorised NLC user, he or she should not participate in or allow unauthorised users to access the network by using NLC IT resources or a personal computer connected to the NLC campus wide Local Area Network (LAN).
- Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
- Without the system owner's or administrator's permission, no user may attempt to access restricted areas of the network, an operating system, security software, or other administrative applications.
- Users must follow the policies and guidelines for each set of resources to which they have been given access. When other policies are more restrictive than this one, the one that is more restrictive takes precedence.

7. Privacy and Personal Rights

1) All NLC IT users are expected to respect the privacy and personal rights of others.
2) Without the authorization and approval of the Competent Authority, do not access or copy another user's email, data, programmes, or other files.
3) While the College does not generally monitor or limit the content of information transmitted over the campus wide LAN, it does reserve the right to access and review such information under certain conditions and with the approval of the appropriate authority.

8. Violation of Policy

Any violation of the basic objectives and areas specified in the College's IT Policy will be considered a violation, as well as a misconduct and gross misconduct under College Rules.

9. Implementation of Policy

The College will establish necessary rules for the implementation of this policy as needed.

10. Email Account Use and Privacy Policy

While every effort is made to protect NLC's email users' privacy, this is not always possible. Because employees are given access to electronic information systems and network services to conduct College business, there may be times when the College reserves and retains the right to access and inspect stored information with the user's consent, based on approval from competent authority.

Staff and faculty may use the email facility of NLC by logging with their User ID and password. For obtaining the institutional email account, user may contact Computer Center/ IT Cell for email account and default password by submitting an application in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the College's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited

bulk email messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

3. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
4. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
5. Impersonating email account of others will be taken as a serious offence under the College IT security policy.

11. Access to the Network and Privacy Policy

11.1 Access to Internet and Intranet

1) Before connecting the client system to the College Campus wide LAN, the user must register the client system and obtain one-time approval from the competent authority.
2) NLC must maintain two independent networks, namely the Internet and the Intranet. There must be no physical connections or devices between the two networks. End point compliance must be implemented on both networks to prevent unauthorized data access.
3) Users shall not engage in any activity that circumvents network filtering via any website or application, nor shall they engage in any other unlawful acts that may endanger the network's performance or security.

11.2 Access to NLC's Wireless Networks

For connecting to a NLC's wireless network, user shall ensure the following:

1) Before connecting an access device to the NLC's wireless network, the user must register the access device and obtain one-time approval from the competent authority.

2) Wireless client systems and wireless devices must be authenticated before connecting to the NLC's wireless access points.

3) To guarantee data security, users should avoid connecting their devices to unsecured wireless networks.

12. Social Media Policy

12.1 Filtering and blocking of sites:

1) The Computer Centre or any other Implementing Agency (IA) may block content on the Internet that is in violation of the IT Act 2000 or other applicable laws, or that poses a security risk to the network.

2) The Computer Centre or any other Implementing Agency (IA) may also block content that, in the College's opinion, is inappropriate or may harm users' productivity.

12.2 Access to Social Media Sites from NLC's Network

1) The "Framework and Guidelines for Use of Social Media for Government Organizations" governs NLC users' use of social networking sites.
2) When posting information on social networking sites, the user must adhere to all applicable provisions of the Information Technology Act of 2000.User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
3) User shall not post any material that is offensive, threatening, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
4) User shall not disclose or use any confidential information obtained in their capacity asan employee of the College.
5) User shall not make any comment or post any material that might otherwise cause damage to NLC's reputation.

13. Video Surveillance Policy

The system has been installed by the College with the primary purpose of reducing the threat of crime generally, protecting college premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders etc.

These purposes will be achieved by monitoring the system to:

1. Assist in the prevention and detection of crime.
2. Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
3. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

14. Monitoring and Privacy

1) From the point of policy compliance, the Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals.
2) The IA/Nodal Agency may access, review, copy, or delete any type of electronic communication or file stored on College provided devices without prior notice to the user for security reasons or to comply with applicable laws. This includes files, e-mails, posts on any electronic media, and Internet history, among other things.
3) IA may monitor user's online activities on NLC network, subject to such Standard Operating Procedures of GoI norms.

15. Use of IT Devices Issued by NLC

IT devices issued by the NLC to a user must be used primarily for academic, research, and other College-related purposes, and in a lawful and ethical manner, Best practices for using desktop devices, portable devices, external storage media, and peripheral devices such as printers and scanners are all covered in this section.

16. Security Incident Management Process

- A security incident is any occurrence that compromises the availability, integrity, confidentiality, or authority of College data. IA reserves the right to deactivate/remove any device from the network if it is deemed a threat that could compromise a system without prior notice to the College's competent authority
- Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA as per the IT Act 2000 and other applicable laws.

17. Deactivation

- In case of any threat to security of NLC's systems or network from the resources beingused by a user, the resources being used may be deactivated immediately by the IA.
- Subsequent to such deactivation, the concerned user and the competent authority of the College shall be informed.

18. Audit of NLC's Network Infrastructure

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

19. Review and Monitoring

The Policy document needs to be reviewed at least once in two years and updated if required, so as to meet the pace of the advancements in the IT related development in the organization. Review of this policy document shall be done by a committee chaired by Principal of the NLC. The other members of the committee shall comprise of Co-coordinators of IT cell, executive Registrar and other members as nominated by the Chair.

20. Additional Activities under IT policy of NLC

20.1 IT Hardware Installation Policy

College network users must take certain precautions when having their computers or peripherals installed in order to experience the least amount of inconvenience due to service interruptions caused by hardware failures.

A. **Who is Primary User**

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. What are End User Computer Systems

Apart from the client PCs used by the users, the College will consider servers not directly administered by Computer Centre, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the Computer Centre, are still considered under this policy as "end- users" computers.

C. Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.

D. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

E. Network Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. Maintenance of Computer Systems provided by the NLC

For all the computers that were purchased by the college centrally and distributed by the Estate Branch, college Computer Maintenance Cell attached with Computer Centre will attend to the complaints related to any maintenance related problems.

20.2 Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, College IT policy does not allow any pirated/unauthorized software installation on the College owned computers and the computers connected to the College campus network. In case of any such instances, College will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. Operating System and its Updating

Individual users should make sure that respective computer systems have their OS 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.

College 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

a. 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.
b. Any software installed should be for activities of the College only.

C. Antivirus Software and its updating

Computer systems used in the College should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

D. Backups of Data

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

20.3 Network (Intranet & Internet) Use Policy

Network connectivity provided through the College, either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the College IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the College's network should be reported to Computer Centre.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the College network, should have an IP address assigned by the Computer Centre. Following a systematic approach, the range of IP addresses that will be allocated will be based on Virtual LAN (VLAN) created against each entity or objective. Any device connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

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

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policyof the College. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the services run by the Computer Centre.

Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. Running Network Services on the Servers

a. Individual departments/individuals connecting to the College network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the Computer Centre in writing and after meeting the requirements of the College IT policy for running such services. Non-compliance with this policy is a direct violation of the College IT policy, and will result in termination of their connection to the Network.

b. Computer Centre takes no responsibility for the content of machines connected to the Network, regardless of those machines being College or personal property.

c. Computer Centre will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

d. Access to remote networks using a College’s network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the College Network connects. College network and computer resources are not to be used for personal commercial purposes.

e. Network traffic will be monitored for security and for performance reasons at Computer Centre.

f. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

D. **Internet Bandwidth obtained by Other Departments**

a. Internet bandwidth acquired by any department of the College under any research programme/project should ideally be pooled with the College's Internet bandwidth, and be treated as College's common resource.
b. Under particular circumstances, which prevent any such pooling with theCollege Internet bandwidth, such network should be totally separated from the College's campus network. All the computer systems using that network should have separate VLANs based on grouping criterion.
c. IP address scheme (private as well as public) and the College gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the College IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to Computer Centre.
d. Non-compliance to this policy will be direct violation of the College's IT security policy.

21 Amendments to Policy

The College reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the NLC website and by continuing to use the College's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

22 Contact Us

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

IT CELL, North Lakhimpur College (Autonomous)

Phone: 9435086753, 7002285761

Email: admin@nlc.ac.in