



IT Policy

Preamble:

Nehru Arts and Science College (NASC) provides and maintains technological products, services and facilities like Personal Computers(PCs), servers, Internet and application software to students and teachers for teaching-learning process. The Information Technology (IT) Policy of the College defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure safety and security of data, products and facilities. It also provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the students and teachers pertaining to technological assets and services.

1. General Rules


All users must comply with Rules, Regulations and Policies, cyber laws, IT Act of Government of India and the terms of (applicable) contracts including software licenses while using NASC IT resources. It may include but not limited to: privacy, copyright, trademark and obscenity; hacking, cracking and similar activities, Scams and pyramid schemes, the NASC Student Code of Conduct etc. Users are responsible for ascertaining the necessary authorizations before using the NASC IT resources. They are responsible for the activities from their accounts. Under any circumstances, Accounts and passwords must not be used by persons other than those to whom they have been assigned by the account administrator. Any detect/suspect of unauthorized use of accounts or resources must be reported to the appropriate account administrator. Users who violate this policy will be subjected to disciplinary action.

2. Purchase

All the IT equipment need to be procured will be purchased by the purchase department through proper channel after the approval of the head of the institution. All computer purchases must be made with the supplier(s) approved by the College and conform to a set of College-specified standard models, with the following exceptions

2.1 Faculty whose teaching and research responsibilities require an alternative to the standard configuration (Must be approved by the Principal)




PRINCIPAL
Nehru Arts and Science College (Autonomous)
Nehru Gardens, Thirumalayampalayam,
Coimbatore - 641 105.



2.2 Administrators and staff whose specific technical, environmental, or functional job responsibilities require an alternative to the standard configuration (must be approved by the Principal)

2.3 All computers purchased with External funds remain the property of the College until disposed of through the Nehru Arts and Science College surplus property programme

3. Management of computers

All the computers are secured using strong password. The passwords were changed in a periodic interval. All desktop computers should have the latest version of antivirus and should retain the setting that schedules regular updates of virus definitions from the central server. All Windows desktops should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default. The password should be difficult to break with a minimum of 8 characters including at least one capital letter, small letter, number and symbol (*!/@/&). The guest account should be disabled. All users are recommended to use in built firewall of windows. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall. All the software on the compromised computer systems should be re-installed from scratch. When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk. Any software installations can be done only in administrator account. Software installation rights of other user accounts are disabled. In addition to the above suggestions, Information Technology Unit (IT Unit) recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

4. Management of Internet Facility

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 Information Technology Unit (IT Unit) is responsible for the ongoing maintenance

and support of the Network, exclusive of local applications. Problems within the College network should be reported to IT UNIT.

All the staff members and students are provided with a unique access ID and password for using college internet through wired (LAN) or wireless (WiFi) network. The user Access ID will not be shared with anyone else. In addition, the Access ID will only be used primarily for educational/official purposes. The User guarantees that the Access ID will always have a password. The user will not share the password or Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the College. Students, staff and faculty who leave the College will have their Access ID and associated files deleted. No User will be allowed more than one Access ID at a time. On behalf of the College, IT Unit reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

5. Licensing and Installation of Software

All computer should have all licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, the College IT policy does not allow any pirated/unauthorized software installation on the college owned computers and the computers connected to the campus network. In case of any such instance, the department/individual shall personally be responsible for any pirated software installed on the computers located in their department/individuals" rooms.

Free and Open Source Software (FOSS) Community is "By the Community, For the Community, of the Community, To the Community on No Profit No Loss Basis. Open Source Software, is and will always remain free. There is no license to pay to anybody." The central and state Governments have introduced policies on the adoption of open source software, which make it mandatory for all software applications and services of the government be built using open source software, so that projects under Digital India "ensure[s] efficiency, transparency and reliability of such services at



affordable costs". The Government realizes that Free Software presents a unique opportunity in building a truly egalitarian knowledge society. Nehru Arts and Science College encourages all members of its community to use FOSS to the extent possible. There is an immense opportunity to select and develop FOSS based on the requirements of the College.

6. IT Security policy

IT Security Incident is an incident that may affect the confidentiality, integrity or availability of the College's IT infrastructure through unauthorized access, accidental disclosure, or other, including:

- 6.1 The presence of any form of malicious software (malware, viruses, worms, etc.).
- 6.2 The presence of any abnormal software that was not previously present on a Computer or Server.
- 6.3 Suspicion that your user account has been compromised.
- 6.4 Intentional or accidental exposure of sensitive information.
- 6.5 Web browsers re-directing automatically or producing popup messages or advertisements unexpectedly.
- 6.6 File types, formats, or naming conventions changing unexpectedly or files not opening as expected.
- 6.7 Slow Computer performance, applications hanging, or any unexpected behaviour.
- 6.8 Notifications that anti-virus or firewalls are not running or are disabled.
- 6.9 Clicking a link, opening an attachment, or providing credentials in response to a suspicious e-mail.
- 6.10 Lost or stolen devices including but not limited to laptops, mobile phones, desktop computers, portable storage devices, switches, etc.
- 6.11 Firewall is deployed to monitor the incoming and outgoing network traffic and to restrict the unauthorized access from outside.

7. CCTV Surveillance

CCTV cameras has been installed by College with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff,




PRINCIPAL
Nehru Arts and Science College (Autonomous)
Nehru Gardens, Thirumalayampalayam,
Coimbatore - 641 105.



students and visitors consistent with respect for the individuals' privacy. Cameras will be located at strategic points on the campus, principally the key areas of institution such as all the gates, entrance, corridor and passage of all blocks, canteen, library, accounts section. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera installation is in use.

8. Email Access

Email ID with institute domain (nehrucolleges.com) will be provided to all staff and students for official communication. For obtaining the College email account, user may contact IT unit for email account and default password. Users need to create a strong password and has to change it in a periodic interval.

In an effort to increase the efficient distribution of critical information to all Faculties, Staff and Students, and the College Administrators, it is recommended to utilize the College e-mail services, for formal College communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal official notices from the College will be communicated to faculty, staff and students through College e-mail. These communications may include administrative content, such as human resources information, policy messages, general College messages, official announcements, etc. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to <http://gmail.com> with their User ID and password by submitting an application in a prescribed format.

9. Backup and Recovery of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. Operating System and other software should be on C



drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on Google drive or CD or other storage devices such as pen drives, External Hard Discs etc.

10. IT asset management

NASC System is committed to managing the lifecycle of its IT assets. IT assets include items such as servers, desktops, laptops, and network devices, as well as software, applications, programs and logical processes. Owners have a duty of care to protect IT assets whether they are in use, stored, or in a state of disposal. All devices purchased with College funding will be inventoried and the inventory is kept up to date. IT assets must be protected against physical or financial loss, whether by theft, mishandling, or accidental damage, either through primary prevention (eg. physical security) or remediation (eg. marking).

11. Server Management

Servers are Computers explicitly purchased to provide services to other Computers on the network. These services include, but are not limited to, file sharing, printing, database access, e-mail, web services, authentication, and any other applications that are accessible via the network. Servers must be secured to the greatest extent possible, including the disabling of all unnecessary services, configuration of file sharing services to provide reasonable and appropriate security and changing of all default passwords. Appropriate backups of the server's OS, applications, data, and configuration documentation must be maintained, with type and frequency of the backups dependent upon the criticality of service(s) hosted.

12. Computer Ethics and Etiquette

The User will not attempt to override or break the security of the College computers, networks, or machines/networks accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk e-mail messages comes under IT



Policy violation. In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

13. Account Termination and Appeal Process

Accounts on College network systems may be terminated or disabled with little or no notice for a periodic time. When an account is terminated or disabled, IT Unit will make an attempt to contact the user through College administrative office and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the IT Unit of the same. But, if the termination of account is on the grounds of will full breach of IT policies of the College / Group by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the Head of the IT Unit, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Head of the College to review the evidence and hear reasons why an appeal should be considered. If the Head of the College recommends revival of the account, it will be enabled. Users may note that the College Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate College/NGI authorities.

14. E- waste Disposal

Electronic waste, also known as E-waste, is electronic products that have outlived their usefulness and are due for disposal. These products have toxic components such as lead, mercury and cadmium. Improper disposal of electronic waste pollutes the environment with hazardous toxins, thereby causing widespread health problems and environmental degradation. The College and group endeavour to ensure environmental conservation and protection from the effects of e- waste. The College recognizes the need to dispose e-waste in a manner that is safe and sound with respect to its staff, students, institutional operations and stakeholders. Any E-waste generated in the campus shall be managed and handled in accordance with the compliance criteria and the procedure laid down in



E-waste (Management & Handling) Rules under the Environment Protection Act 2016 and E- Waste (Management) Amendment Rules, 2018.

15. Disclaimer

Security is neither perfect nor permanent. This is even more true for Information and IT infrastructure where change is the only constant - systems change, requirements change, new bugs are discovered, new vulnerabilities are disclosed, new threats arise, old vulnerabilities take new forms - all this as the information and the equipment go through their lifecycles from creation and use to destruction, and from great value for the organization to none. In this Dynamic environment, this document attempts to bring some long-lasting order and balance. Owing to the very nature of its subject, this document, too, is neither perfect nor permanent. The document must necessarily be periodically updated for it to remain effective.