Amala College of Nursing

Amala Nagar, Thrissur - 680555

Information Technology (IT) Policy

TERMINOLOGY

IT policies may be classified into following groups:

IT Hardware Installation Policy

Software Installation and Licensing Policy

Network (Intranet & Internet) Use Policy

E-mail Account Use Policy

Database Use Policy

Further, the policies will be applicable at two levels:

End Users Groups (Faculty, students, Senior administrators, Officers and other staff]

Network Administrators

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the ACON IT policy. Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by Amala College of Nursing, Thrissur by any member may even result in disciplinary action against the offender by the authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

Students: UG, PG, Research

Employees (Permanent/Temporary/Contractual)

Faculty Administrative Staff (Non-Technical/Technical)

Higher Authorities and Officers

Guests Resources

Network Devices wired/wireless

Internet Access

Official Websites, web applications

Official Email services

Data Storage

PURCHASE

1. The Administrative department has set procedures & guidelines need to be followed to purchase new technological equipment, services or software for official purposes.
2. All approved equipment, services or software will be purchased through the Procurement Dept., unless informed/permitted otherwise., complying with Govt. regulations.
3. IT Dept. will assist the Procurement Dept while evaluating best and most cost- effective hardware or software to be purchased for a particular dept./project/purpose based on the requirement. The IT Dept. will also make sure all hardware/software standards defined in the IT Policy are enforced during such purchases.
4. Complete details related to purchase of technological equipment services or software can be found in the Procurement Policy Manual.

COMPLIANCE

1. All departments are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the institute.
2. Any employee who notices misuse or improper use of equipment or software within the organization must inform Engineer-(Infrastructure and maintenance) immediately.
3. Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the Management Committee of the Institute.

EMPLOYEE TRAINING

1. Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software.
2. Management will conduct an IT training on a regular or requirement basis.

IT SUPPORT

1. Employees may need hardware/software installations or may face technological issues which cannot be resolved on their own. Employees are expected to get help from the IT Dept. for such issues IT Support Email ID.
2. For the sake of quick understanding employees are expected to provide details of their issue or help required in the Ticket raised or Support Email sent
3. For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all employees to inform the IT Dept.
4. For any damage to Personal Computers, approval from Laboratory Assistant would be required for PC replacement
5. After raising a query in the System, employees should expect a reply from the IT Dept. within 1 working day. The IT Dept, may ask the employee to deposit the problematic equipment to the IT

Dept. for checking and will inform the timeline for repair/maintenance/troubleshooting/installations or the required work.

6. If there is no response in 1 working day, then the IT Dept. Designated Staff should be asked for an explanation for the delay. If no response is obtained in 3 working days, a complaint can be raised through an email to the Principal.
7. Query will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the IT Team

EQUIPMENT USAGE POLICY

Equipment Purchase

1. The following equipment is purchased by the organization and provided to individual employees, departments or projects for their official use.
2. The list can be modified as and when required.
    a) Personal Computing Devices (Desktop, Laptop, Tablet)
    b) Computer Peripherals (Printer, Scanner. Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, Modem etc.)
    c) Networking Equipment & Supplies (Router, Switch, Antenna, Wiring, etc.)
    d) Cell phones e. Biometric Devices
3. The finance department procedures & guidelines need to be followed to purchase new equipment for official purposes. All approved equipment will be purchased through the IT department unless permitted otherwise.
4. The IT Dept. will maintain a small inventory of standard PCs, software and equipment required frequently to minimize delay in fulfilling critical orders.

Inventory Management

1. The IT Dept is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the organization.
2. The following information is to be maintained for above mentioned assets in an

Inventory Sheet:

a. Item
b. Brand/ Company Name
c. Serial Number d. Basic Configuration (eg HP Laptop, 120 GB HD, 2 GB RAM etc.)
d. Physical Location
e. Date of Purchase
f. Purchase Cost
g. Current Person In-Charge

3. Proper information about all technological assets provided to a specific department, project or center must be regularly maintained in their respective Inventory Sheets by an assigned coordinator on a regular basis. The information thus maintained must be shared with the IT Dept as and when requested.
4. When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.
5. All technological assets of the organization must be physically tagged with codes for easy identification.
6. Periodic inventory audits will be carried out by the IT Dept to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

Equipment Allocation, De-allocation & Relocation

1. Alloration of Assets:

a) New Employees may be allocated a personal computer (desktop or laptop) for office work on the Day of Joining, as per work requirement.
b) If required, employees can request Head, IT Department for additional equipment or supplies like external keyboard, mouse etc.
c) Allocation of additional assets to an employee is at the sole discretion of the Head, IT Department.
d) No employee is allowed to carry official electronic devices out of office without permission from Principal.

2) De-allocation of Assets:

a) It is the Head, IT Department responsibility to collect all allocated organizational equipment & other assets from an employee who is leaving the organization.
b) Updating the Inventory Sheet is mandatory after receiving back all allocated equipment.
c) The received assets must be returned back to the Administration Dept.

Equipment Usage, Maintenance and Security

1. It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.
2. Proper guidelines or safety information must be obtained from designated staff in the IT Dept. before operating any equipment for the first time.
3. Any observed malfunction, error, fault or problem while operating any equipment. owned by the organization or assigned to you must be immediately informed to the designated staff in IT Dept.

4. Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.
5. If your assigned computer devise is malfunctioning or underperforming and needs to be replaced or repaired, then written approval HOD is required for the same. The malfunctioning device needs to be submitted to the IT Dept for checking, maintenance or repair. The IT Dept. staff person will give a time estimate for repair/maintenance.
6. The HOD can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT Dept. The issue will then be resolved by HOD in consultation with the IT Dept. Head. The Principal can be consulted in terms of serious disputes or unresolved issues.

Phone Usage Policy

1. Landline phone systems are installed in the organization's offices to communicateinternally with other employees and make external calls.
2. The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.
3. The Admin, Dept, is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted.
4. Employees should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.

PERSONAL COMPUTER (PC) STANDARDS

General Guidelines

1. It is the responsibility of the IT Dept. to establish and maintain standard configurations of hardware and software for PCs owned by the organization. The standard, can however, be modified at any point in time as required by the IT Dept. Head in consultation with the Principal.
2. Multiple configurations are maintained as per the different requirements of various departments and projects in the organization, in consultation with the HOD.
3. Only in exceptional cases, when none of the standard configurations satisfy the work requirements, can an employee request a non-standard PC configuration. Valid reasons need to be provided for the request and written approval of Head IT department is required for the same.

Network Access

1. All PCs being used in the organization are enabled to connect to the connect to the organization’s Local Area Network as well as the Internet.
2. Network security is enabled in all PCs through Firewall, Web Security and Email Security software.

3. Employees are expected to undertake appropriate security measures as enlisted in the IT Policy.

Hardware Installation Policy

The network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

End User Computer Systems

Apart from the client PCs used by the users, the College will consider servers not directly administered by INTERNET UNIT, 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 INTERNET UNIT, are still considered under this policy as "end users" computers,

Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably be under comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include 08 re-installation and checking virus related problems also.

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. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

Network Access

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.

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.

Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written Intimation to the Central Lab Administration as they maintain a record of computer Identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified.

Noncompliance

ACON faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's noncompliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole College

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, ACON IT policy does not allow any pirated/unauthorized campus network. In case of any such instances, Amala College of Nursing , Thrissur will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/Individuals' rooms

Operating System and its Updating

Individual users who has the privilege to update the software should make sure that respective computer systems have their US updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to for them.

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. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically

no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

Data Backup Procedure

1. Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that employees keep important official data in some external storage device also.
2. File Backup System: a. Organization will be installing a file server for backing up data of all employees. All employees are expected to keep official data on the file system.
3. Employee's Reporting Manager or the Management Committee or the IT Manager will have access to that data c. All employees will login to the file server through ADDCI user ID and password.
4. Server backup: a. IT Dept. is expected to maintain an incremental backup of all servers with at least 4 copies of all servers. At any time, backups of all servers must he maintained. b. Replica mode of all running servers will be offline and it should maintain half hourly backup

INTERNET USAGE POLICY

Network (Intranet & Internet) Use Policy

Network connectivity provided through the institution, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the ACON IT Policy. The Communication & Information Services (INTERNET UNIT) 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 INTERNET UNIT.

Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any Section, department of the college under any research program /project should ideally he pooled with the college's Internet bandwidth, and he treated as college's common resource.

Email Account Use Policy.

General Guidelines

1. Internet is a paid resource and therefore shall be used only for office work
2. The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
3. The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received The

Administration committee can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.

4. The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.

Internet Login Guidelines

1. All employees may be provided with a Username and Password to login to the Internet network in the office and to monitor their individual usage.
2. An employee can also get a local static IP address for internet and intranet use. All employees will be responsible for the internet usage through this local static IP.
3. Username and password for a new employee must be requested by the administration Dept.
4. Sharing the Username and Password with another employee, visitor or guest user is prohibited.
5. A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.
6. The IT Dept. will define guidelines for issuing new passwords or allowing employees to modify their own passwords.
7. Any password security breach must be notified to the IT Dept. immediately
8. Username and password allotted to an employee will be deleted upon resignation /termination / retirement from the organization.

Online Content Usage Guidelines

1. Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site Immediately.
2. During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.
3. 3) Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.
4. Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

Inappropriate Use

The following activities are prohibited on organization's Internet network.

This list can be modified/updated anytime by the Management Committee as deemed fit. Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

1. Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
2. Downloading images, videos and documents unless required to official work.
3. Accessing, displaying, uploading, downloading, staring, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work
4. Accessing pirated software, tools or data using the official network or systems
5. Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee
6. Engaging in any criminal or illegal activity or violating law 8) Invading privacy of coworkers
7. Using the Internet for personal financial gain or for conducting personal business
8. Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
9. Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation

INFORMATION SECURITY POLICY

General Guidelines

1. Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.
2. Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs
3. Appropriate training must be provided to data owners, data users, and network & system administrators to ensure data security

Data Classification

1. The organization classifies data into three categories:

a. High Risk

   i. It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure.
   ii. Eg :Payroll, personnel, financial, biometric data.

b. Medium Risk:

i. It includes confidential data which would not impose losses on the organization if disclosed, but is also not publicly available
ii. Eg Agreement documents, unpublished reports, etc.

c. Low Risk:

i. It includes information that can be freely disseminated Eg brochures,published reports, other printed material etc.

2. Different protection strategies must be developed by the IT department for the above three data categories. Information about the same must be disseminatedappropriately to all relevant departments and staff
3. High risk data must be encrypted when transmitted over insecure channels.
4. All data must be backed up on a regular basis as per the rules defined by the IT Dept, at that time

Access Control

1. Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication Includes the use of passwords, biometrics or other recognized forms of authentication.
2. All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.
3. Default passwords on all systems must be changed after installation. 4. Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.

Virus Prevention

1. Virus prevention for personal computers and email usage has been described previously.
2. Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.
3. Whenever feasible, system/network administrators must inform users when at virus/other vulnerability has been detected in the network or systems.

Intrusion Detection.

1. Intrusion detection must be implemented on all servers and workstations containing high and medium risk data.
2. Operating system and application software logging process must be enabled on all systems.
3. Server, firewall and critical system logs must be reviewed frequently.

EMAIL & CHAT POLICY

General Guidelines

1. The organization reserves the right to approve or disapprove which electronic messaging systems and chat platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for office use only.
2. An employee who, upon joining the organization, is provided with an official email address should use it for official purposes only.
3. Any email security breach must be notified to the IT Dept. Immediately.
4. Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.
5. All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication.
6. Electronic mails and messages should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.
7. All email signatures must have appropriate designations of employees and must be in the format approved by the Management Committee.

Ownership

1. The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the organization.
2. The organization reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems
3. The organization reserves the right to alter, modify, re-route or block messages as deemed appropriate
4. IT Administrator can change the email system password and monitor email usage of any employee for security purposes.

Confidentiality

1. Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Reporting Manager(s) and/or the Management Committee.
2. Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.

3. Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
4. Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

Email Security

1. Anti-Virus:
   a) Anti-virus software pre-approved by the Dept. Head IT should be installed in the laptop/desktop provided to a new employee after Joining the organization.
   b) All employees in the organization are expected to make sure they have anti-virus software installed in their laptops/desktops (personal or official) used for office work.
   c) Organization will hear responsibility for providing installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop provided by the organization. The employee is responsible for installing good quality anti-virus software in their personal laptop/ desktop used for office work.
   d) Employees are prohibited from disabling the anti-virus software on organization provided laptops/desktops.
   e) Employees should make sure their anti-virus is regularly updated and not out of date.

2. Safe Email Usage:
   1) Following precautions must be taken to maintain email security
      a) Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
      b) In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment
      c) Use Email spam filters to filter out spam emails.

Inappropriate Use

a) Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.
b) Official Email platforms or electronic messaging systems should not be used for personal work personal gain or the promotion or publication of one's religious, social or political views.
c) Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

SOFTWARE USAGE POLICY

General Guidelines

a) Third-party software (free as well as purchased) required for day-to-day work will be preinstalled onto all company systems before handing them over to employees. A designated person in the IT Dept. can be contacted to add to/delete from the list of pre-installed software on organizational computers.
b) No other third-party software free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept.
c) To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email.
d) Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

Compliance

a) No employee is allowed to install pirated software on official compating systems
b) Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.
c) Any duplication, ilegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action,
d) The Procurement Dept. procedures & guidelines need to be followed to purchase new software (commercial or shareware) for official purposes. All approved software will be purchased through the Procurement Dept, unless informed/permitted otherwise
e) Any employee who notices misuse or improper use of software within the organization must inform his/her Reporting Manager(s).

Software Registration

a) Software licensed or purchased by the organization must be registered in the name of the organization with the Job Role or Department in which it will be used and not in the name of an individual.
b) After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the IT Dept.
c) After installation, all original installation media (CDs, DVDs, etc.) must be safely stared in a designated location by the IT Dept.

Software Audit

a) The IT Dept. will conduct periodic audit of software installed in all company owned systems to make sure all compliances are being met.
b) Prior notice may or may not be provided by the IT Dept. before conducting the
c) Software Audit.
d) During this audit, the IT Dept. will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes.
e) The full cooperation of all employees is required during such audits.

E-waste policy

Amala college of nursing, Thrissur is committed towards making the world a better place to live through designing process which will help to reduce the e-Waste management challenges. The e waste disposal is done in three different ways

Buyback scheme:-

Electronic waste, such as batteries and electronic devices, are part of buy-back-schemes and are replaced with new hardware.

Used for Training:-

Old computers and processors from the various departments like labs/classrooms/office are sent to the hardware-lab of the college, where students learn hardware assembling and studies on components.

Recycling of Waste:-

Initiatives are taken by students and faculty to up-cycle waste material as decoration-items for fests/events on campus

E-waste disposal:-

Vendors who take E-waste collect the materials which are to be dumped. Usable items are given free-of-cost to Needy people in the neighborhood