DE PAUL INSTITUTE OF SCIENCE & TECHNOLOGY, ANGAMALY (DiST)

IT POLICY

1.0 Introduction

De Paul Institute of Science & Technology (DiST) provides Information Technology (IT) facilities to support the teaching learning, research and administrative functions of the college and to enhance efficiency in these realms. Intranet and internet resources have become most important resources in educational institutions and research organizations. These resources are tools to access and process information in their areas of work. When using these facilities there is the need to ensure legal and appropriate use of IT. IT policy of DiST covers the guidelines and ethical behaviour that should be followed when these assets are accessed, created, managed or controlled by the stakeholders in the college. Information assets in this policy document data, information, systems, computers, network devices and documents.

Total bandwidth available in DiST is 150 mbps. Hence, when users are given free access to internet, non-essential downloads is likely to affect the traffic resulting in poor quality of service which will critically affect the users. Since the computer systems are networked, viruses entering the system through downloads may affect the whole system and a lot of critical files may be corrupted. Hence, running the campus management intranet 'Dicoman', developed in-house, and internet is entrusted with the IT department under the leadership of the administrator. This department ensures the smooth running of the firewall security, proxy, DNS, email, web and application servers and managing the network of the college. Uncontrolled browsing may lead to lowering the quality of work, choking of available bandwidth, and exposure to legal liability and cases of sexual harassment, confidential information being made public, etc. The IT policy of the college is framed in order to convince the users regarding the guidelines to be followed when using the IT infrastructure of the college even though some may feel these restrictions are unwarranted. While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users.

1.1 Objectives

- To provide all required IT resources including new technologies which will benefit the students, staff and administration.
- To have an annual plan of introducing new technologies in line with the new developments.
- To develop a plan for annual maintenance of existing IT infrastructure.
- To make sure that the IT infrastructure is used most efficiently.

- To control and manage the use in such a way that uncontrolled surfing for purposes other than that which is envisaged is not happening.
- To convince the users regarding the guidelines to be followed.
- To ensure that there is proper balance of security and the ability to conduct the rightful functions by the users.

1.2 Coverage of DiST IT Policy

This IT policy applies to technology administered by the college centrally or by the departments, to individuals of the DiST community or to the resident or non-resident visitors to the college on their computers connected to the college network. It also applies to the resources administered by the different departments such as library, computer centers, laboratories, offices and hostels where the network facility is available. Computers owned by individuals when connected to the campus network should follow the guidelines given in this policy. All the students, faculty, staff, departments, visiting faculty and others who are granted permission to use this network should comply with the policy directions. Resources of the institute include network devices, wired or wireless, internet access, official websites, web applications, official e-mail services, data storage, mobile/desktop/server computing facility, documentation facility (printers/scanners) and multimedia contents.

Any violations of this policy by any user stated above may end up in disciplinary actions including enforcement of law for illegal action.

1.2.1 IT Hardware Installation Policy

- The users in the Institute have to observe certain precautions while getting their computers and peripherals installed so that it creates minimum interruption due to hardware failures.
- Computers purchased by the college should preferably be with 3-year onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.
- 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. Furthermore, these UPS

systems should be connected to the electrical points that are provided with proper earthing system and have properly laid electrical wiring.

- 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 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.
- Any computer system may be moved from one location to another with prior written intimation from the IT department as they maintain a record of computer identification names and corresponding IP address.
- 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 computers, etc. An individual's noncompliant computer can have significant, adverse effects on other individuals, groups, departments, or even the whole college.
- IT department, upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and direct him to bring into compliance. Such notification will be done via email/telephone.

1.2.2 Software Installation and Licensing Policy

- The IT department of the college has to make sure that all computers purchased have 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/unauthorised software installation on the college owned computers and the computers connected to the campus network.
- The IT department should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and

Servers). Checking for updates and updating of the OS should be performed at least once in a week or so.

- The 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.
- Computer systems used in the college should have anti-virus software installed, and it should be active at all times.
- 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. In case of any virus problem it should be intimated to the IT department. Users should keep their valuable data either on CD or other storage devices such as pen drives.

1.2.3 Intranet and Internet Use Policy

Network connectivity provided through the college, referred to hereafter as "the Network", is governed under the college IT Policy. The IT department is responsible for the ongoing maintenance and support of the Network. Problems within the network should be reported to the IT department. This department will be forced to disconnect computers connected to the college network where potentially damaging software is found to exist. Similarly a device may also be disconnected if the activity adversely affects the Network's performance. College network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons by the IT department. Impersonation of an authorised user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

1.2.4 Email Account Use Policy

In order to distribute the critical information to all faculties, staff and students, it is better to utilise the college e-mail services, for formal college communication and for academic and other official purposes. This will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal communications may include administrative content, such as human resources information, policy messages, general messages, official announcements, etc. To receive these notices, it is essential that the e-mail address be

kept active by using it regularly. Students, staff and faculty will be given DiST domain User ID and password by the IT department at the time of joining the college.

The users should adhere to the following guidelines.

a) This ID should be used primarily for academic and official purposes.
b) Using this ID for illegal/commercial purposes is a direct violation of the IT policy of the college. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages and generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
c) All users should keep the mail box used space within about 80% usage threshold
d) Users should not open any mail or attachment that is from unknown and suspicious source or suspicious material from known sources.
e) 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.
f) Users should refrain from trying to break into others' email accounts, as it is infringing the privacy of other users.
g) Users should be careful to sign out of their accounts while using the computers that are shared by other users as well.
h) Impersonating email account of others will be taken as a serious offence under the IT security policy.
i) Confidential and sensitive information about the organization or its employees should not be exchanged with anybody without formal written approval from the principal.
j) Unauthorized copying and sharing of the copyrighted content of the college is strictly prohibited.
k) Employees and students should not give their username and password to guests. If required, they will be given guest user id and password by the IT department.
l) Official e mail account should not be used to send derogatory, pornographic, sexual, racist, harassing and offensive material.
m) Official e mail accounts should not be used for personal work, personal gain or promotion of one's religious, social and political views.

1.3 College Data Base

College data base is a vital and important resource for providing useful information from the point of view of e-governance.

This policy relates to the databases maintained by the college administration. Its use must be protected even when the data may not be confidential. DiST is the owner of all the institutional data generated in the college. Individual departments generate these data and they have to be maintained by them. The ultimate data administration is entrusted with the IT department of the college.

College Data should not be shared with anybody outside the college. All database including those collected by the departments, individuals and faculty is for internal use only. Only those data base that is required to perform one's official responsibilities can be accessed by him. Data that will help to directly identify a person or his/her personal information will not be shared with any outsiders including all official agencies without proper sanction from the Principal. Requests from any courts will be forwarded to the Principal and the departments should not respond to that. Requests from law enforcement authorities should also be forwarded to the Principal. Information should not be shared outside for any commercial, marketing solicitation or other purposes. All reports to the University, AICTE and other government agencies will be prepared/compiled and submitted by the Principal's office. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:

a) Modifying/deleting the data items or software components by using illegal access methods.
b) Modifying/deleting the data items or software components deliberately with ulterior motives even by authorised individuals/ departments.
c) Causing database or hardware or system software crash, thereby destroying the whole or part of database deliberately with ulterior motives by any individual.
d) Trying to break security of the Database servers.

Such data tampering actions will result in disciplinary action against the offender by the college authorities. If the matter involves illegal action, law enforcement agencies may become involved.

1.4 Responsibilities of the IT Department

- IT Department monitors the network to ensure that the services are used properly. It provides net access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the college. The campus network and Internet facilities are available 24 hours a day, 7 days a week. All network failures and excess utilisation are reported to the IT department and the department will take care of the problem resolution.
- On monitoring the traffic patterns in the campus network, if it is felt that network security, integrity or network performance is compromised, it will analyse the net traffic offending actions and such equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if required, a report will be sent to higher authorities in case the offences are of very serious nature. For implementing network policy and technology standards the department can take reasonable steps to ensure compliance.
- The IT department, upon receiving complaints from the users regarding difficulties in accessing network due to network related problems, should make sure that it coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.
- IT department will disconnect any department or individuals from the network whose internet traffic violates practices set forth in this policy.
- Maintenance of computer hardware and peripherals that are either under warranty or annual maintenance contract is entrusted to this department.
- The IT department in the college will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased and was loaded by the company. The IT department should not encourage installing any unauthorised software on the computer systems of the users. If this department comes across any applications that are interfering with the network operations or with the IT policies of the college, such incidents should be brought to the notice of the college authorities. When the IT department reformats the computer systems and re-install OS and other application software, users should be informed sufficiently in advance so that they securely move the files.
- The IT department has to make sure that the configurations in the hardware and software are standard ones.

1.5 Preservation of Network Equipment and Accessories

Routers, switches, connecting inlets to the network, racks, UPS and their batteries that are installed at different locations are the property of the college and are maintained by the IT department. Tampering with any of these items by users comes under violation of IT policy.

1.6 Responsibilities of the Administrative Units

To provide network and other IT facilities to the new members of the college and for withdrawal of these facilities from those who are leaving the institute and also for keeping the web site up-to-date in respect of its contents the IT department should be given up to date information by the administrative unit. This information may be about new appointments, promotions, new enrollments, on the expiry of studentship, removal of names from the rolls, important events, developments, achievements, etc.

1.7 Compliance

All users of the computer network in the college should strictly follow the guidelines of this policy. If somebody notices any improper use of the IT facilities by any user it should be immediately reported to the IT department. Improper use of equipment and software by any user will attract disciplinary actions.

1.8 IT Training

Every year there may be upgradation or changes in the software and network installations. During holidays, IT department may bring changes or additions to the existing system. Hence, training will be given to all the employees of the college, preferably, in the beginning of the year by the IT department. The subsidiary staff will also be given training on the basics of using computers and logging on to internet and e mail.

New students joining the college will be given training regarding how to use the college network system.

1.9 IT support

Employees in need of IT support related to hardware or software have to approach the IT department in the college. They should not try to rectify the problems on their own as it may lead to damage to the hardware.

1.10 Inventory Management

The IT department is responsible for maintaining a systematic record of all the hardware, software and other equipment related to IT use. Information regarding item, brand and company name, serial number, basic configuration, physical location, date of purchase, purchase price and current person in charge should be properly recorded by the IT department.

Departments should also maintain proper inventory records of the equipment given to them. The HOD will be responsible for entrusting a person in the department for inventory management.

All technological assets of the institution must be tagged for easy identification. The IT department should carry out periodical audit in the departments to make sure that these assets are in proper condition.

If there are any complaints regarding the working condition of these assets, it should be intimated to the IT department by recording it in the complaint register maintained in the front office. The IT department has to make sure that the complaints are attended to in time. No employee is allowed to take any of the equipment of the college home, without the written permission from the Principal. Any equipment that is allotted to an employee should be returned to the IT department at the time of leaving the institution.

1.11 Bring Your Own Device (BYOD)

Recently, the college has introduced the policy of bring your own device (BYOD). As per this policy, the faculty members can purchase their own computer systems and the college will provide Rs. 5000/ per year per person for three years for maintenance of these devices. If they are in need of funds for purchase of new laptop, the college will give an advance of Rs. 15000/ which will be repaid in one year by the faculty. With the introduction of this policy the personal computers given to the faculty in their cabins will be taken back by the college. The faculty should take their own laptops for classes as there will not be any more laptops in the department. Other equipments will be available as usual.