IT POLICY

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar-Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

TABLE OF CONTENTS

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar-Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

IT POLICY

1. NEED FOR IT POLICY

IT policies are pivotal in the success of any organization. They define what personnel has responsibility of what information within the company. IT policies shape organizations' preparedness and response to security incidents. Information security relies on well- documented policies that are acknowledged and followed by all members of an organization.

IT security policies should outline rules for user and IT personnel behavior, while also identifying consequences for not adhering to them. Policies should define the main risks within the organization and provide guidelines on how to reduce these risks. Policies should be customized based on the organization's valuable assets and biggest risks.

The most important policies apply to all users of the organization's information systems. These policies protect the confidentiality, integrity, and availability of systems and data. While policies can be altered, shortened, or combined with others, the following policies should be implemented in all organizations.

CLASSIFICATION OF IT POLICIES

1. **IT hardware Installation Policy**
2. **Software Installation and License Policy**
3. **Network [Internet] Use Policy**
4. **E-mail Account Use Policy**
5. **Web Site Hosting Policy**
6. **College Database Use Policy**

Further, the policies shall be applicable at two levels:

1. End Users Groups (Faculty, students, Administrators, Officers and other staff)
2. Network Administrators

It may be noted that the IT Policy applies to technology administered by the college centrally, or by the individual departments, to information services provided by the college administration, or by the individual departments, or by individuals of the college community, or by authorized resident or non-resident visitors on their own hardware connected to the college.

This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centre's, Laboratories, Offices of the college and recognized sub units of the college and wherever the network facility was provided by the college.

Computers owned by the individuals, or those owned by research projects of the faculty and students when connected to campus network are subjected to the 'Do's and 'Don'ts detailed in the 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 of the college, must comply with the guidelines. Certain violations of IT policy by any member of the college community may even result in disciplinary action against the offender/s by the college authorities. If the matter requires the involvement of legal action, law enforcement agencies may also be informed.

Applies to stakeholders on campus or off campus:

- Students:
- 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
- Mobile/Desktop/server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents, Surveillance network
- Learning Management Systems
- Other governing software, etc.

2. IT HARDWARE INSTALLATION POLICY

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

A. Who is the Primary User: An individual in whose room the computer is installed and is used primarily by him/her is considered to be the "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. End User of Computer Systems: Apart from the client PCs, 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.

C. Warranty and Annual Maintenance Contract: Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS reinstallation and checking virus related problems also. Department HODs should monitor for the proper and timely maintenance.

D. Power Connection to Computers and Peripherals: All the computers and peripherals should be connected to the electrical point strictly through UPS if available. 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.

E. Network Cable Connection: While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they might 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 the network, they should be protected with password and also with 'read only' access rule.

G. Shifting Computer from One Location to another: Computer system may be moved from one location to another with prior written intimation to the Network Unit, as Network Unit maintains a record of computer identification names (MAC Address, and Serial Number) and corresponding IP address. Such computer identification names follow the convention that comprises the Department name abbreviation and serial number. As and when any deviation (from the list maintained by Network Unit) is found for any computer system, network connection would be disabled and the same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs the Network Unit in writing/by email, connection will be restored.

H. Maintenance of Computer Systems provided by the College: For all the computers that are purchased by the college, Computer Maintenance Cell (COMPUTER CENTRE) will attend to the complaints related to any maintenance related problems.

I. Noncompliance: Faculty, staff, and students who do not comply 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 and inoperable computers, resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, or even whole departments. Hence it is critical to bring all computers into compliance as soon as they are recognized as non-compliant.

J. Internet Unit/Computer Centre Interface: Upon finding a non-compliant computer affecting the network INTERNET UNIT will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTRE, if applicable. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT shall provide guidance as needed for the individual to gain compliance.

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar-Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

3. SOFTWARE INSTALLATION AND LICENSING POLICY

Any computer purchase 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.

Promoting Free and Open Source Software (FOSS)

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. The Government realizes that Free Software presents a unique opportunity in building a truly egalitarian knowledge society. Our 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.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through the 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 are periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

2. Our College has made it a policy to encourage its user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

3. Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a monthly. Even if the systems are configured for automatic updates, it is the users' responsibility to make sure that the updates are being done properly.

B. Antivirus Software and its updating

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar-Vepemkulam Road,
Thaichanallur, Tirunelveli - 627 358.

1. 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.

2. Individual users should make sure that respective computer systems have current virus protection software (windows defender) installed and maintained. He/she should make sure that the software is running correctly.

C. Backups 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. OS and other software should be on C drive and user's data files on the D drive and file server. 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 foolproof solution. Apart from this, users should keep their valuable data either on an external storage device or Google Drive for data integration.

D. Noncompliance

Our College faculty, staff, and students who are not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files, inoperable computer resulting in loss of productivity, risk of spread of infection to others or confidential data being revealed to unauthorized persons. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even the whole college. Hence it is critical to bring all computers into compliance as soon as they are recognized as non-compliant.

E. Internet Unit/Computer Centre Interface

INTERNET UNIT upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user shall follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar-Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358.

4. NETWORK (INTRANET AND INTERNET) USE POLICY

Network connectivity provided through the College, referred to hereafter as "the Network", either through an authenticated network access connection, is governed under the College 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 network should be reported to INTERNET UNIT.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the network, should have an IP address assigned by the INTERNET UNIT. Following a systematic approach, the range of IP addresses that will be allocated to each group is decided. So, any computer connected to the network from that group will be allocated an IP address only from that Address pool. Further, each network port in the room from where that computer is 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, the concerned user can approach and get the IP address from the INTERNET UNIT.

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 addresses are given to the computers.

B. DHCP Configuration by Individual Department /Section/ User

Use of any computer at the 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 an absolute violation of IP address allocation policy of the college.

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

Individual departments/individuals connecting to the network over the LAN may run server software, e.g., google domain server based E-mail id's and FTP server, only after bringing it to the knowledge of the INTRANET UNIT 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.

INTERNET UNIT takes no responsibility for the content of machines connected to the Network, regardless of whether those machines belong to the college or individuals. INTERNET UNIT 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. Access to remote networks using college 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. Network traffic will be monitored for security and for performance reasons at INTERNET UNIT. Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

D. Broadband/ Leased Line Connections

Computer systems that are part of the campus-wide network, whether property of the college or personal property, should not be used for broadband/ Leased Line connections.

E. Wireless Local Area Networks

This policy applies, in its entirety, to the department, or division of wireless local area networks. In addition to the requirements of this policy, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.

F. Wireless Access Policies

Service is provided via Wi-Fi "access points," which are located throughout the majority of buildings and some outdoor areas across campuses.

Wi-Fi bandwidth is shared by everyone connected to a given access point and/or other wireless devices operating in the same area.

To promote efficient and secure Wi-Fi network access these standards and their related restrictions are outlined in further detail below.

Wi-Fi IP Address Policy

- DHCP is the standard addressing method for the Wi-Fi networks, and it is expected to meet the majority of customer requirements.
- Wi-Fi is a dynamic service. Due to the dynamic nature of Wi-Fi, IP space serving a building or open space can, and will, change over time due to capacity re-engineering.
- Wi-Fi Fixed IP addresses are available for clients with a demonstrated needs. These clients should understand that due to the dynamic nature of Wi-Fi address space, they may be required to change these addresses periodically and possibly with short notice.

5. EMAIL ACCOUNT USE POLICY

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the college administrators, it is recommended to utilize the college email services, for formal communication and for academic and other official purposes. Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal communications are official notices from the college to staff. These 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 email address be kept active by using it regularly. For obtaining the college's email account, the user may contact INTERNET UNIT 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 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 e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature

or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.

6. Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox onto their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
7. 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.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the college IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of college's email usage policy.
12. Any Spam mail received by the user into INBOX should be forwarded to info@tec-edu.in
13. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to info@tec-edu.infor necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.
14. Use of the computing services and facilities of the college for political purposes is banned.

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepenkulam Road,
Thalchanallur, Tirunelveli - 627 358.

6. WEB SITE HOSTING POLICY

a) Official Pages

Departments, Cells, central facilities may have pages on College official Web Site. As on date, the Computer Center is responsible for maintaining the official web site of the institute viz.,https://cellname@tec-edu.in/

b) Personal Pages

It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the institute by sending a written request or mail to Computer Center giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the institute.

However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

c) Responsibilities for updating Web Pages

Departments, cell, and individuals are responsible to send updated information time to time about their Web pages to Computer Center.

7. COLLEGE DATABASE USE POLICY

This Policy relates to the databases maintained by the institute. Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential.

Our college has its own policies regarding the creation of database and access to information and amore generic policy on data access. Combined, these policies outline the institute's approach to both the access and use of this institute resource.

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Chidambaranagar - Vepemkulam Road,
Thatchanallur, Tirunelveli - 627 358

Database Ownership:

College is the data owner of the entire Institute's institutional data generated in the institute.

Data Administrators:

Data administration activities outlined may be delegated to some of the officers in that department.

MIS Components:

For the purpose of Management Information System requirements of the institute these are:

- Employee Information Management System.
- Students Information Management System.
- Financial Information Management System.
- Library Management System.
- Document Management & Information Retrieval System.

Here are some general policy guidelines and parameters for departments, cells and administrative department data users.

8. VIDEO SURVEILLANCE POLICY (CCTV)

The College is fully committed to operating a safe environment, it therefore has in place a **CLOSED CIRCUIT TELEVISION ("CCTV")** system to assist in providing a safe and secure environment for students, staff and visitors, as well as protect College property.

CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Data Protection Act 1998, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation.

The College will have due regard to the Data Protection Act 1998, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

The College system comprises a number of fixed and dome cameras located both internally and externally around the College sites. All cameras maybe monitored and are only available for use by approved members of staff.

The CCTV system is owned by the College and will be subject to review on an annual basis.

The purpose of this Policy is to regulate the management, operation and use of the CCTV system at the College.

Purpose of CCTV

The College has installed a CCTV system to:

- To increase the personal safety of staff and students and reduce the fear of physical abuse, intimidation and crime
- Protect College buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption
- To support the Police in a bid to deter and detect crime
- Assist in prevention and detection of crime
- Assist with the identification, apprehension and prosecution of offenders
- Assist with the identification of actions/activities that might result in disciplinary proceedings against staff and students
- Monitor security of campus buildings

The system will be provided and operated in a way that is consistent with an individual's right to privacy.

Covert Recording

Prior to authorization the requesting applicant must have demonstrated and documented that all reasonable procedures and practices were put in place to prevent suspected illegal or unauthorized activity from taking place.

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal, inappropriate or unauthorized activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom. The College may require legal advice in approving and assessing the need for covert recording in all instances.

Covert cameras may be used under the following circumstances on the written or electronic authorization of the Chief Operating Officer.

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording
- That there is reasonable cause to suspect that illegal activity is taking place or is about to take place or the inappropriate or unauthorized activity is taking place; that may seriously or substantially affect the operation or reputation of the College

Unless required for evidential purposes or the investigation of crime or otherwise required by law, covertly recorded images will be retained for no longer than 31 days from the date of recording. A record of data destruction will be made in confirmation on the authorized request to make covert recordings.

The CCTV system will not be used to:

- Provide images to the world wide web
- Record sound
- Disclose to the media

Operation

The CCTV surveillance system is owned by the College.Cameras will be used to monitor activities within the College buildings and other areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the occupants within the College grounds, together with its visitors.

Materials or knowledge secured as a result of CCTV system will not be used for any commercial purpose.

Downloads will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Downloads will never be released to the media for purposes of entertainment. The planning and design of the existing CCTV system has endeavored to ensure that

the CCTV system will give maximum effectiveness and efficiency but it is not possible to guarantee that the CCTV system will cover or detect every single incident taking place in the areas of coverage.

Overview of System

The CCTV system runs 24 hours a day, 7 days a week. The CCTV system comprises fixed position cameras; pan tilt and zoom cameras; monitors; multiplexers; digital recorders and public information signs. CCTV cameras are located at strategic points on site, principally at the entrance and exit point for the sites and various buildings, as well as main thoroughfares and common areas throughout the sites.

CCTV signs will be prominently placed at strategic points and at entrance and exit points of the college sites to inform staff, students, visitors and members of the public that a CCTV installation is in use, its purpose and details of the operator. Although every effort has been made to ensure maximum effectiveness of the CCTV system; it does not cover all areas and it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Access to Images

Individual Access Rights

The General Data Protection Regulation gives individuals the right to access personal information about themselves, including CCTV images. All requests for access to view/copy CCTV footage by individuals should be made in writing to the College's Data Controller through concerned HoD and Principal. Requests for access to CCTV images must include:

- The reason for the request
- The date and time the images were recorded
- Information to identify the individual, if necessary
- The location of the CCTV camera
- Proof of Identity

The College will respond promptly and at the latest within 30 calendar days of receiving the request processing fee, determined by the Chief Operating Officer and sufficient information to identify the images requested. If the College cannot comply with the request, the reasons will be documented.

The requester will be advised of these in writing, where possible.

Access to Images by Third Parties

Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under the GDPR, and care must be taken when complying with such requests to ensure that neither the GDPR, HRA or the CCTV Policy are breached.

As noted above, requests from third parties will only be granted if the requestor satisfies the following criteria:

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution Agencies and their Legal Representatives
- Insurance Companies and their Legal Representatives

All third party requests for access to a copy of CCTV footage should be made in writing to the College's Data Controller. A law enforcement or prosecution agency is requesting access they should make a request in accordance with the General Data Protection Regulations.

Retention and Disposal

Recorded images will be retained for no longer than 31 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

All images on electronic storage will be erased by automated system overwriting. All downloads, still photographs and hard copy prints will be securely disposed of as confidential waste. The date and method of destruction will be recorded on the bottom of the original approval to copy held by the Security Manager.

Do's

1. Do respect the rule "That which is not expressively permitted is prohibited".
2. Do use the internet only for academic related matters
3. Do check the information you access is accurate, complete and current.
4. Do respect the legal protections to data and software provided by copyright and licenses.
5. Do inform the concerned authority in case of any unusual occurrence..

6. Do contact the concerned authority in case of any Internet related problems.
7. Do clean the browser history and cache periodically.
8. Do sign off from captive portal when you are not using Internet or leaving the system

Don'ts

1. Do not download content from Internet sites unless it is related to your work.
2. Do not make any unauthorized entry into any computer or network.
3. Do not represent yourself as another person. Do not share your password.
4. Do not use Internet services to transmit confidential, political, threatening, obscene or harassing materials.
5. Do not attach/transmit files through email which contains illegal/unauthorized materials.
6. Do not use network for Peer to peer file sharing.
7. Do not download any image/video/file which contain pornographic, racist, violence or any illegal activity.
8. Do not use Internet services to download movies/previews/Games.

PRINCIPAL
THAMIRABHARANI ENGINEERING COLLEGE
Chathirampudukulam Village,
Vepamkulam Road,
Tirunelveli - 627 358