VASANTDADA PATIL PRATISHTHAN'S COLLEGE OF ENGINEERING AND VISUAL ARTS
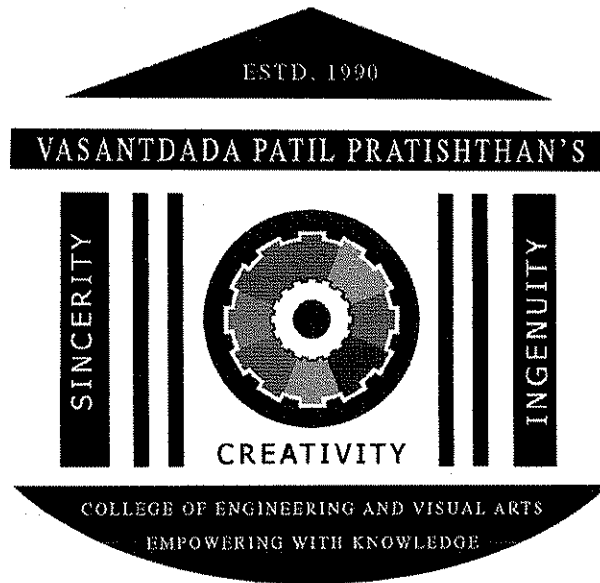

IT POLICY AND GUIDELINES

INDEX

1. Introduction

Vasantdada Patil Pratishthan's College of Engineering and Visual Arts (VPPCOE&VA) is an engineering and technology institute which provides IT resources to support the educational, instructional and administrative activities of the institution and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner.

This document establishes specific requirements for the use of all IT resources at VPPCOE&VA. This policy applies to all users of computing resources owned or managed by VPPCOE&VA. Individuals covered by the policy include VPPCOE&VA faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, any other entity which fall under the management of Vasantdada Patil Pratishthan's College of Engineering and Visual Arts accessing network services via VPPCOE&VA computing facilities.

For the purpose of this policy, the term "IT Resources" includes all institution owned, licensed, or managed hardware and software, and use of the institution network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources can result in unwanted risk and liabilities for the institution. It is, therefore, expected that these resources are used primarily for institution related purposes and in a lawful and ethical way.

2. Purpose and Benefits

This policy defines the mandatory minimum information security requirements for the entity as defined below in scope. Any entity may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets; manage the risk of security exposure or compromise ;assure a secure and stable information technology (IT) environment; identify and respond to events involving information asset misuse, loss or unauthorized disclosure; monitor systems for anomalies that might indicate compromise; and promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure of our institute; compromise data; and result in legal and regulatory non-compliance.

This policy benefits entities by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.
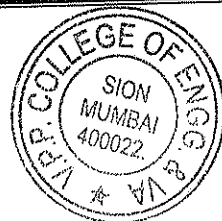
3. Abbreviation

Sr. No.	Abbreviation	Description
1.	VPPCOE&VA	Vasantdada Patil Pratishthan's College of Engineering and Visual Arts
2.	CA	Competent Authority
3.	WAN	Wide Area Network
4.	IA	Implementing Agency
5.	LAN	Local Area Network
6.	GoI	Government of India
7.	IT	Information Technology
8.	ICT	Information and Communication Technology
9.	IP	Internet Protocol
10.	DHCP	Dynamic Host Configuration Protocol
11.	IR	Institutional Repository
12.	CAPEX	Capital Expenditure
13.	OPEX	Operational Expenditure

4. Scope

This policy encompasses all systems, automated and manual, for which the entity has administrative responsibility, including systems managed by entity. It addresses all information, regardless of the form or format, which is created or used in support of institute activities.
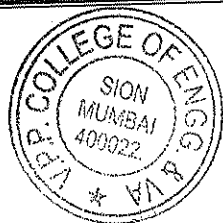
5. Objective

The objective of this policy is to ensure proper access to and usage of VPPCOE&VA's IT resources and prevent their misuse by the users. Use of resources provided by VPPCOE&VA implies the user's agreement to be governed by this policy.

Institution's IT policy exists to maintain, secure, and ensure legal and appropriate use of information technology infrastructure established by the institution on the campus.

This policy establishes Institution-wide strategies and responsibilities for protecting the confidentiality, integrity and availability of the information assets that are accessed, created, managed, and/or controlled by the institution.

Information assets addressed by the policy include data, information systems, computers, network devices as well as documents and verbally communicated information.

6. Roles and Responsibilities

The following roles and responsibilities are envisaged from the entity respectively.

- Manages all the activities relating to the Computer systems and networking.

- Looks after the repair and maintenance of Computer systems and their networking.

- Prepares a schedule for providing computer services to all the concerned.

- Arranges for availability of Internet connection wherever required.

- Arranges computer training /refresher courses for the staff to update their knowledge.

- Maintains and updates the institute's website.

- Manages the firewall, the information system (ERP)
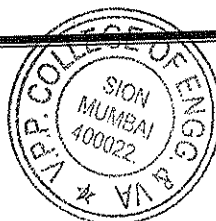
7. Acceptable Use

An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account, or attempt to capture or guess other users' passwords.

A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the institution for all use of such resources. As an authorized VPPCOE&VA user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of VPPCOE&VA or a personal computer that is connected to the VPPCOE&VA campus wide Local Area Network (LAN).

Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access. No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

8. Privacy and Personal Rights

All users of the institution's IT resources are expected to respect the privacy and personal rights of others. Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).

9. Privacy in Email

While every effort is made to ensure the privacy of VPPCOE&VA email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct institution business, there may be instances when the institution, based on approval from competent authority, reserves and retains the right to access and inspect stored information with the consent of the user.

10. User Compliance

When an individual uses VPPCOE&VA"s IT resources, and accepts any Institution issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of VPPCOE&VA and adapt to those changes as necessary from time to time.

11. Access to the Network

11.1. Access to Internet and Intranet

A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the Institution Campus wide LAN.

VPPCOE&VA shall maintain two independent networks, i.e. Internet and Intranet. Both the networks shall not have any physical connection/devices between them. End point compliance shall be implemented on both the networks to prevent unauthorized access to data.

Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

11.2. Access to VPPCOE&VA Wireless Networks

For connecting to a VPPCOE&VA"s wireless network, user shall ensure the following:

A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the VPPCOE&VA"s wireless network. Wireless client systems and wireless devices shall not be allowed to connect to the VPPCOE&VA"s wireless access points without due authentication. To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

11.3. Filtering and blocking of sites

Gajshield/ZYXEL Content Filtering Service (CFS) running on Gajshield/ZYXEL Unified Threat Management and next generation firewalls (NGFWs) is a powerful protection and productivity solution that delivers unequaled content filtering enforcement for educational institutions. Using Gajshield/ZYXEL CFS, organizations has control over the websites students and employees can access using their IT-issued computer behind the firewall.

CFS provides administrators with the tools to create and apply policies that allow or deny access to sites based on individual or group identity.

12. Monitoring and Privacy

Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

IA/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on Institution provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.

IA may monitor user's online activities on Institution network, subject to such Standard Operating Procedures of GoI norms.

13. E-mail Access from the Institution Network

E-mail service authorized by VPPCOE&VA and implemented by the Computer Centre shall only be used for all official correspondence.

More details in this regard are provided in the "E-mail Usage Policy of "VPPCOE&VA".

14. Access to Social Media Sites from VPPCOE&VA Network

Use of social networking sites by VPPCOE&VA users is governed by "Framework and Guidelines for use of Social Media for VPPCOE&VA". User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites. User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws. User shall report any suspicious incident as soon as possible to the competent authority. User shall always use high security settings on social networking sites. User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful. User shall not disclose or use any confidential information obtained in their capacity as an employee of the institution. User shall not make any comment or post any material that might otherwise cause damage to VPPCOE&VA"s reputation.

15. Use of IT Devices Issued by VPPCOE&VA

IT devices issued by the VPPCOE&VA to a user shall be primarily used for academic and any other institution related purposes and in a lawful and ethical way. This applies to practices related to use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

16. Security Incident Management Process

A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of institution's data.

IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the Institution.

Any security incident noticed must immediately be brought to the notice of the IA.

IA shall neither accept nor act on the request from any other organization for scrutiny or release of logs.

17. Intellectual Property

Material accessible through the VPPCOE&VA"s network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use VPPCOE&VA"s network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

18. Enforcement

This policy is applicable to all the users of VPPCOE&VA as specified in Scope of this document. It is mandatory for all users to adhere to the provisions of this policy.

Each entity of VPPCOE&VA shall be responsible for ensuring compliance with the provisions of this policy.

19. Deactivation

In case of any threat to security of VPPCOE&VA"s systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.
Subsequent to such deactivation, the concerned user and the competent authority of the institution shall be informed.

20. VPPCOE&VA Network Diagram

VASANTDADA PATIL PRATISHTHAN'S
COLLEGE OF ENGINEERING & VISUAL ARTS

GROUND FLOOR PLAN
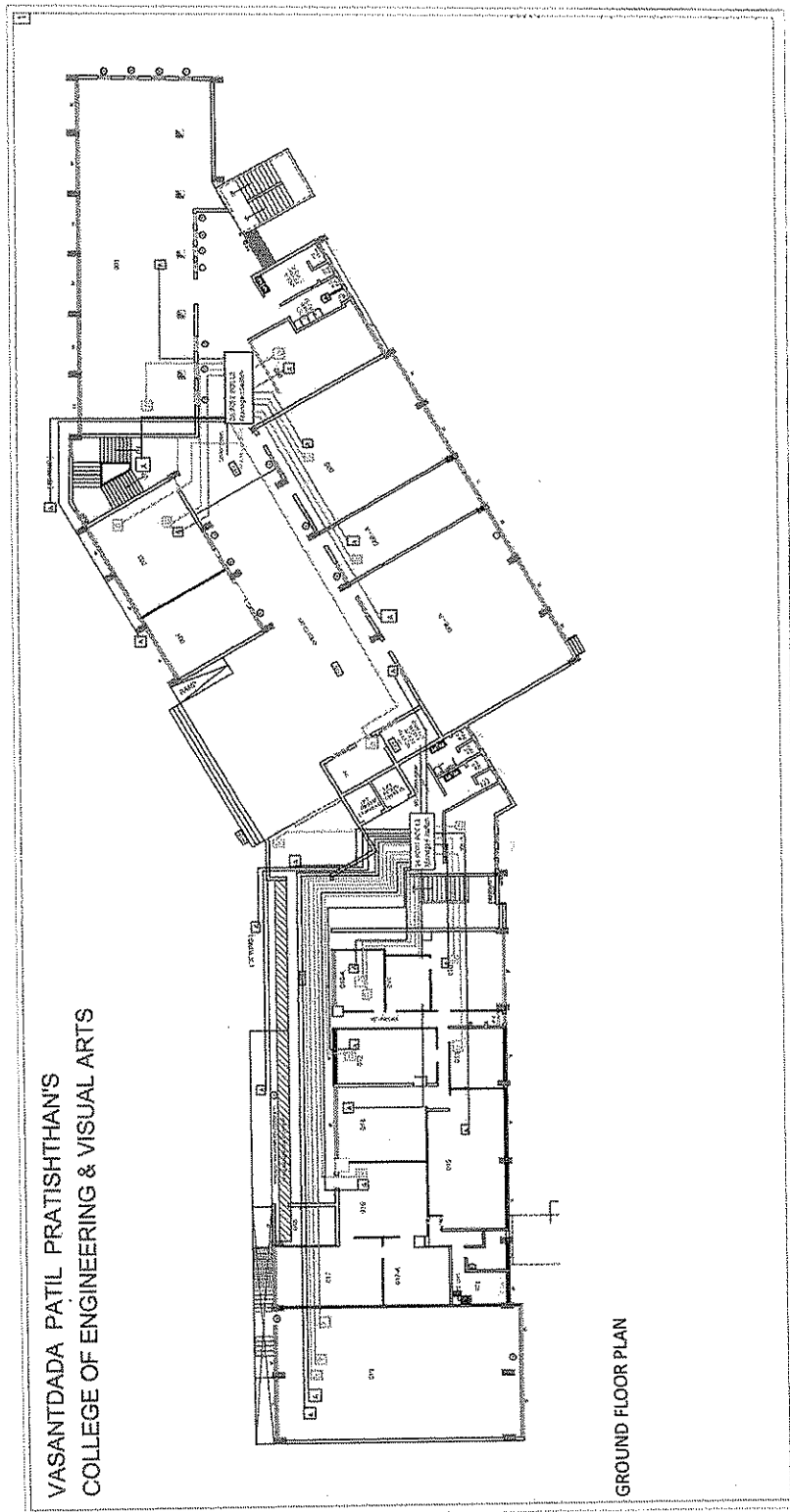
VASANTDADA PATIL PRATISHTHAN'S
COLLEGE OF ENGINEERING & VISUAL ARTS

FIRST FLOOR PLAN

VASANTDADA PATIL PRATISHTHAN'S
COLLEGE OF ENGINEERING & VISUAL ARTS

SECOND FLOOR PLAN

VASANTDADA PATIL PRATISHTHAN'S
COLLEGE OF ENGINEERING & VISUAL ARTS

THIRD FLOOR PLAN

VASANTDADA PATIL PRATISHTHAN'S
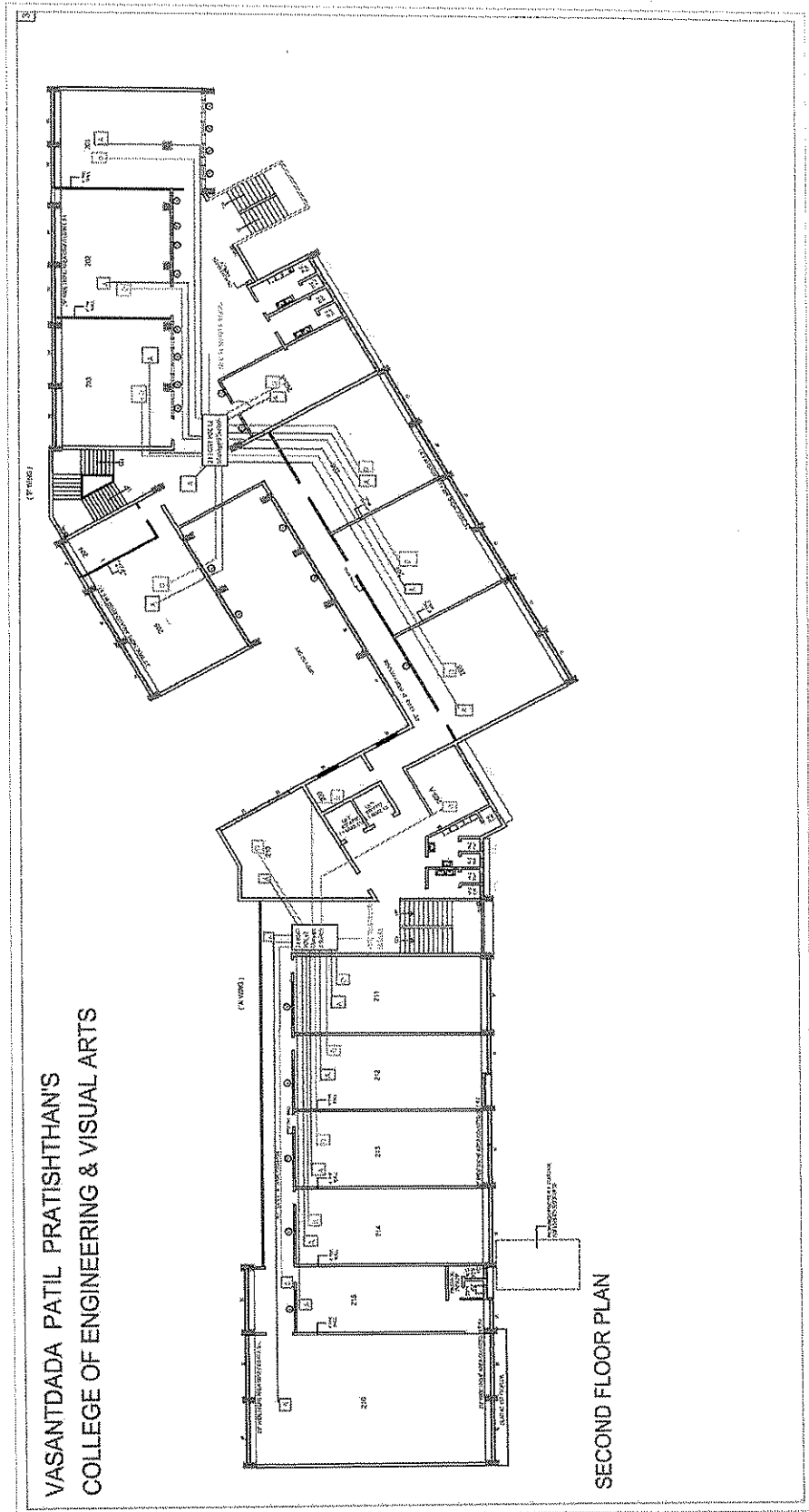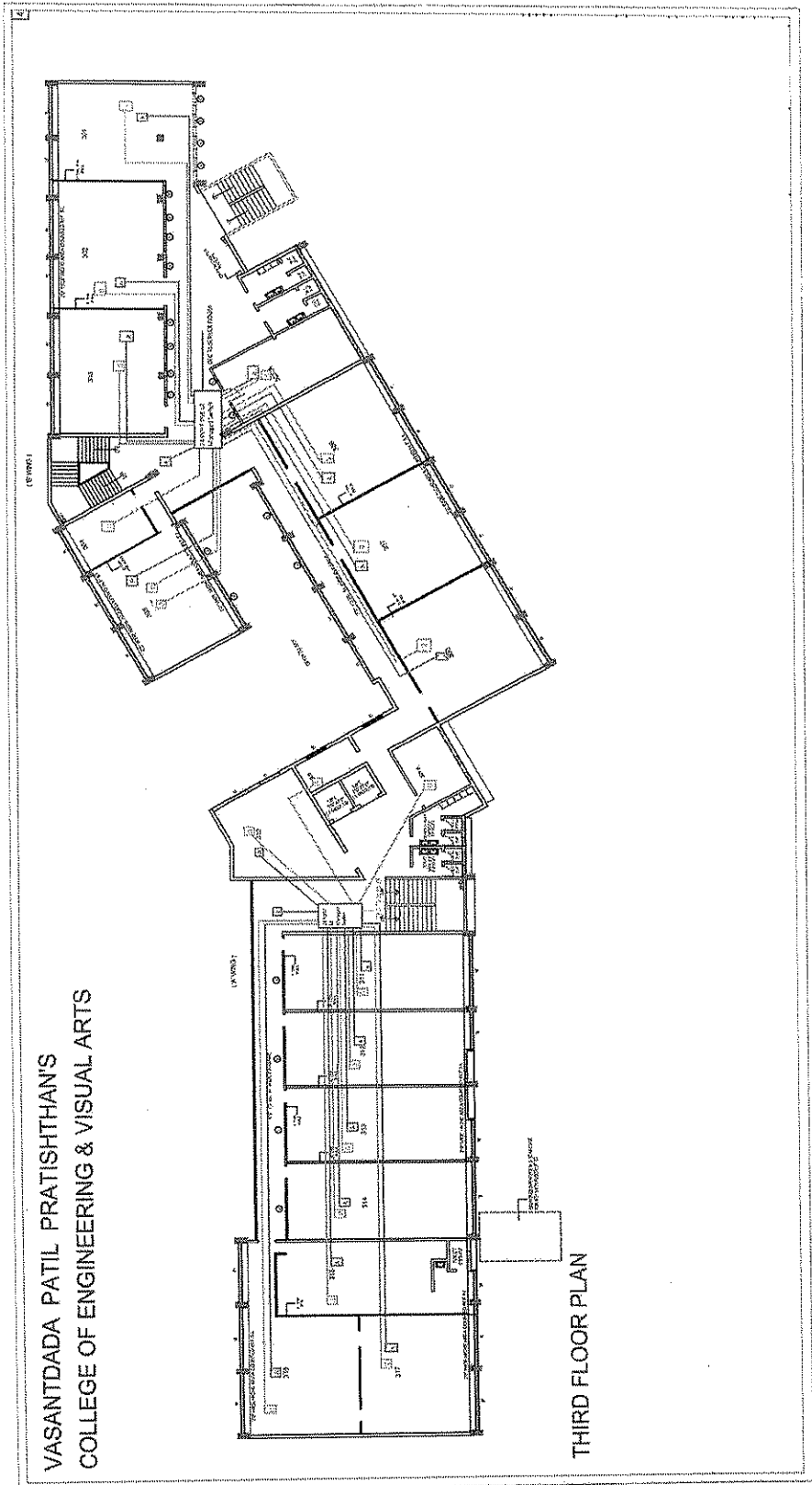COLLEGE OF ENGINEERING & VISUAL ARTS
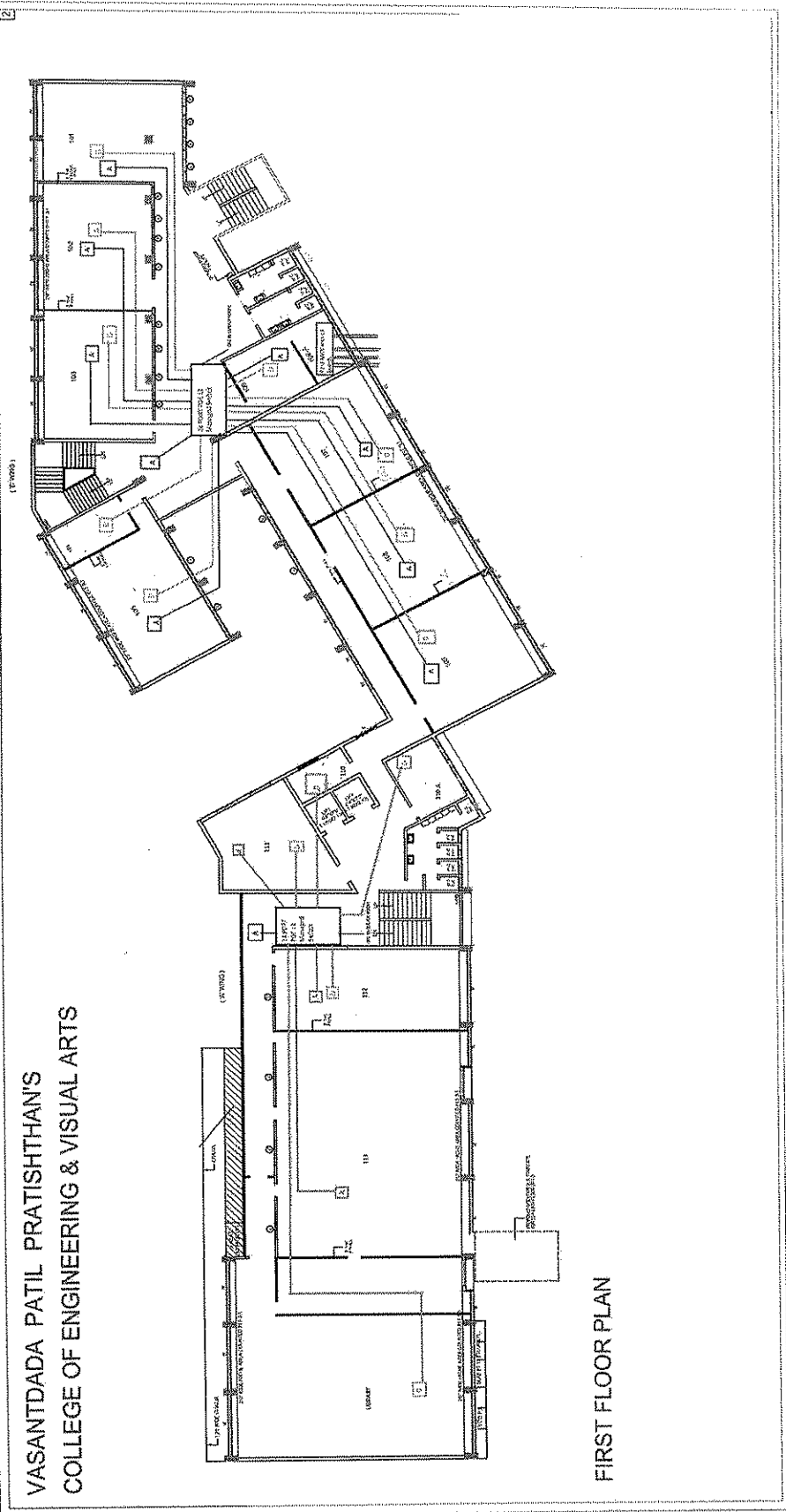
FOURTH FLOOR PLAN

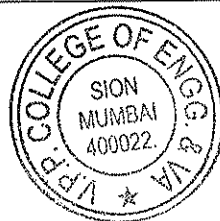VASANTDADA PATIL PRATISHTHAN'S
COLLEGE OF ENGINEERING & VISUAL ARTS
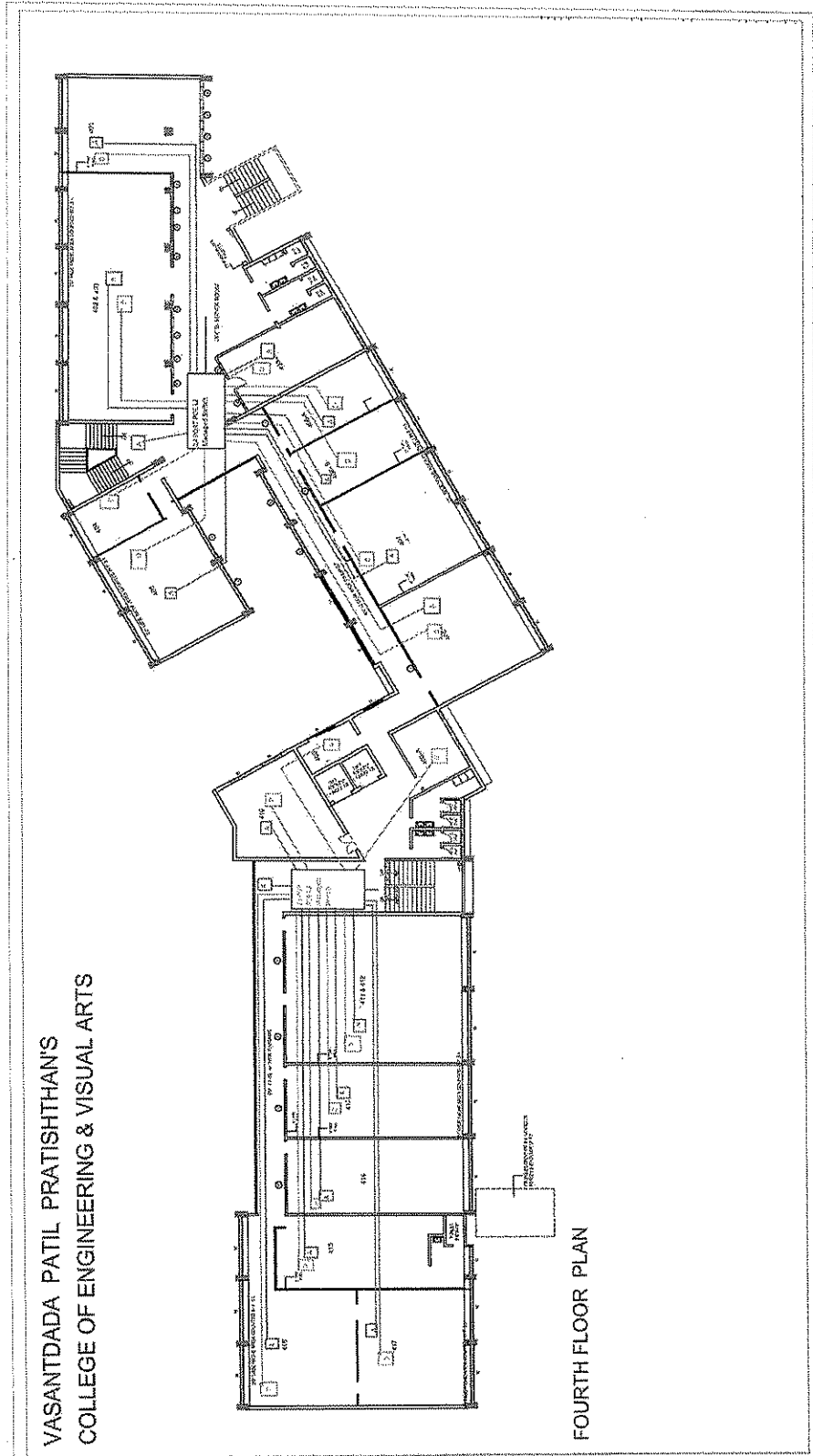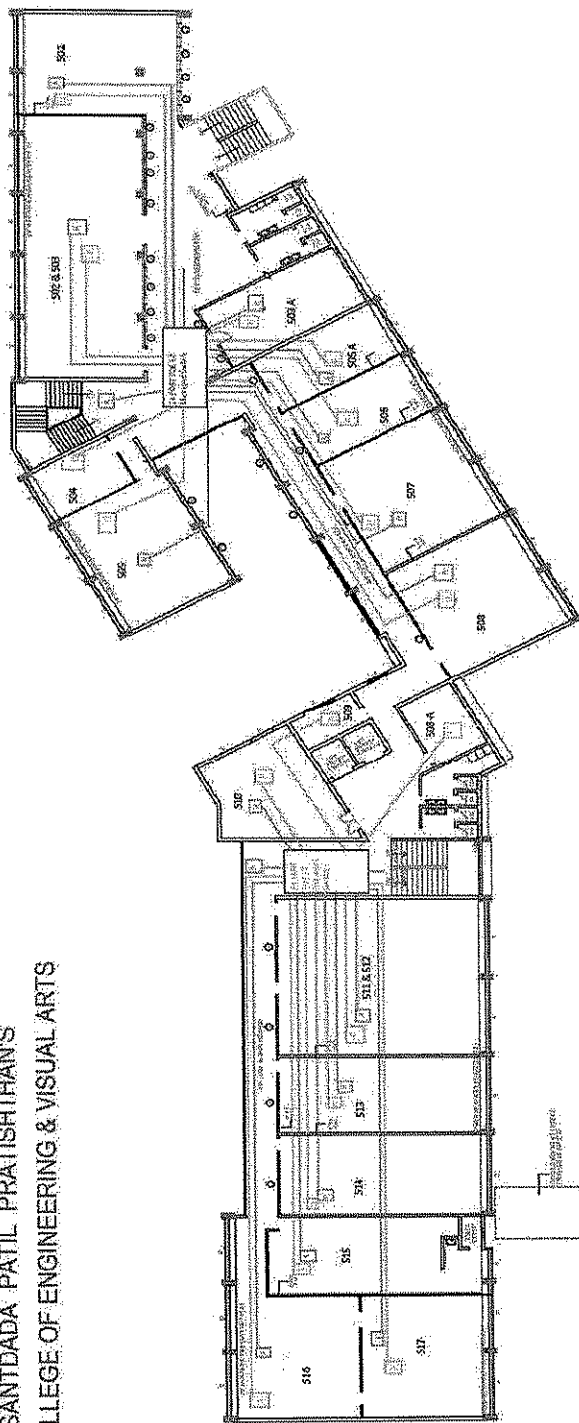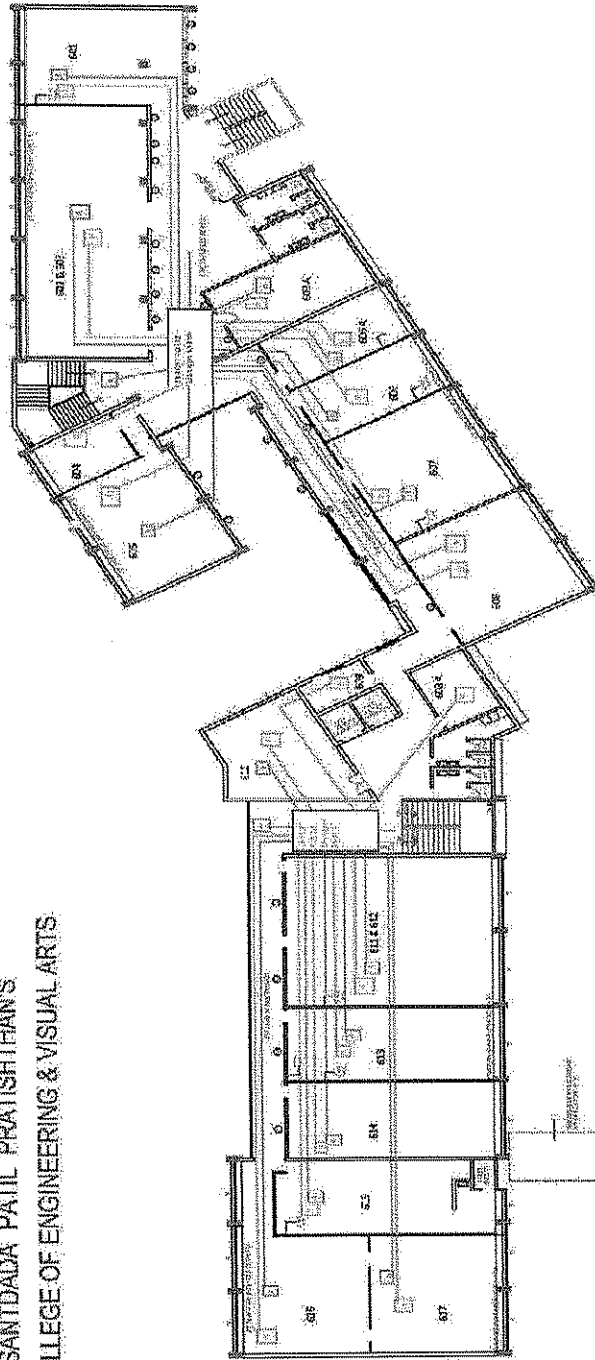
FIFTH FLOOR PLAN

VASANTDADA PATIL PRATISHTHAN'S
COLLEGE OF ENGINEERING & VISUAL ARTS

SIXTH FLOOR PLAN

21. Audit of VPPCOE&VA Network Infrastructure

- The security audit of VPPCOE&VA network infrastructure shall be conducted periodically twice a year by the department of system admin.
- It control security system & risk mitigation.
- Antivirus software & it's updating.

Review:

Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee (ICT) with the approval of the Competent Authority of the institution.

22. IT Hardware Installation Policy

Institution 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.

Primary User: An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user.

Annual Maintenance Contract: Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures.

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

Maintenance of Computer Systems provided by the Institution:
For all the computers that were purchased by the institution centrally the department of system admin will attend to the complaints related to any maintenance related problems.
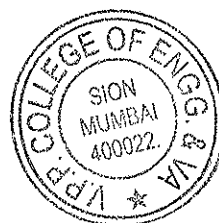
23. Software Installation and Licensing Policy

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.

Operating System and its Updating:

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in 6 months.

Institution as a policy encourages user community to go for open source software such as Ubuntu, Open office to be used on their systems wherever possible.

Use of software on Desktop systems:

Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.

Any software installed should be for activities of the Institution only.

Antivirus Software and its updating:

Computer systems used in the Institution 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.

Backups of Data:

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

24. Use of IT Devices on VPPCOE&VA Network

This section provides the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on VPPCOE&VA's network.

Desktop Devices:

Use and Ownership Desktops shall normally be used only for transacting Institution's works. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

Sharing of data:

Users shall not share their account(s), passwords, digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

Use of Portable devices:

Devices covered under this section include VPPCOE&VA issued machines, laptops etc. Use of the devices shall be governed by the following:

- User shall be held responsible for any unauthorized usage of their VPPCOE&VA issued access device by a third party.

- Users shall keep the VPPCOE&VA issued devices with them at all times or store them in a secured location when not in use. User should not leave the devices unattended in public locations (e.g. classrooms, meeting rooms, restaurants etc.).

- User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy of the application.

- Computer Centre shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible.

- Users shall wipe or securely delete data from the device before returning/ disposing it off.

- Lost, stolen, or misplaced devices shall be immediately reported to the IA/ and the competent authority.
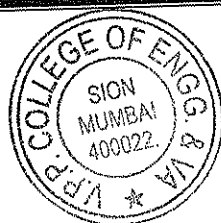
25. Security and Proprietary Information

- User shall take prior approval from the IA to connect any access device to the VPPCOE&VA's network.

- User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy of the application.

- All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.

- Users shall ensure that updated virus-scanning software is running on institute's system. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

- User shall report any loss of data or accessories to the IA and competent authority of VPPCOE&VA.

- Users shall properly shut down the systems before leaving the office/ department.

- Users shall abide by instructions or procedures as directed by the Computer Centre from time to time.

If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the IA (Computer Centre) for corrective action.

26. 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 Institution IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institution"s network should be reported to Computer Centre.

IP Address Allocation:

Any computer (PC/Server) that will be connected to the Institution network, should have an IP address assigned by the Computer Centre. In a specific range any device connected to the network will be allocated IP address only from this range. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

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

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port.

DHCP and Proxy Configuration by Individual Departments /Sections/ Users:

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

Running Network Services on the Servers:

Individual departments/individuals connecting to the Institution network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the Computer Centre in writing and after meeting the requirements of the Institution IT policy for running such services.

Computer Centre takes no responsibility for the content of machines connected to the Network, regardless of those machines being Institution or personal property.
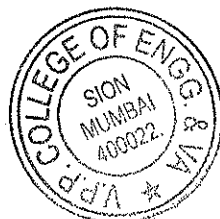
Computer Centre will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the network's performance.

Network traffic will be monitored for security and for performance reasons at Computer Centre. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

Internet Bandwidth obtained by Other Departments:

Internet bandwidth acquired by any department of the Institution under any work should ideally be pooled with the institution's Internet bandwidth, and be treated as institution's common resource.
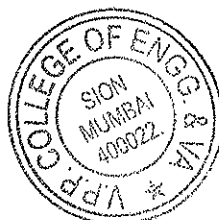
27. Email Account Usage Policy

VPPCOE&VA provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staffs and students, it is recommended to avail official email with VPPCOE&VA domain.

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the institution's administrators, it is recommended to utilize the institution's e-mail services, for formal institution 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 institution communications are official notices from the institution to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institution 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. For obtaining the institution's email account, user may contact Computer Centre for email account and default password by submitting an application in a prescribed Performa.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies: The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

Using the facility for illegal/commercial purposes is a direct violation of the institution's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

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.
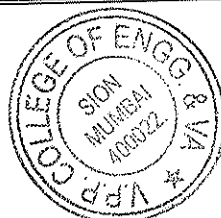
User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious in nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very 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.

User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

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.

Impersonating email account of others will be taken as a serious offence under the IT security policy.

It is ultimately each individual's responsibility to keep their e-mail account free from violations of institution's email usage policy.

28. Disposal of ICT equipment

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the Institution.
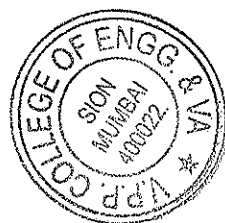
29. Budgetary provisions for ICT

Budgetary provisions should be made under recurring grants (OPEX) to maintain the entire existing ICT infrastructure for smooth functioning of all the ICT enabled services.

Adequate budgetary provisions under capital head (CAPEX) should be kept for up gradation and augmentation of ICT infrastructure

Budgetary provisions under capital grants should also be allocated for implementation of newer ICT solutions from time to time.

30. Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk pvppcoe.system@gmail.com / vppcoe.system@pvppcoe.ac.in on receipt of notice (or where the Institution otherwise becomes aware) of any suspected breach of this Policy, the Institution reserves the right to suspend a user's access to institution's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the Institution's disciplinary procedures.

31. Revisions to Policy

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

32. Contact Us

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

Phone: 9673746340

Email: pvppcoe.system@gmail.com
        vppcoe.system@pvppcoe.ac.in
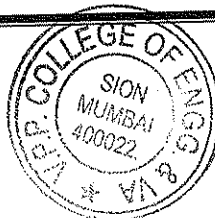
E-mail Requisition Form

Form for Requisition of Official Email Id-

(For Faculty & Staff only)

First Name :	
Middle Name :	
Last Name :	
Department/ Branch :	
Current Email address :	
Mobile Number :	

Note:

Please spell the names and all other information sought above correctly.

This Email address should be currently used by you.

The filled in form should be submitted after getting duly signed from respective Head of the Department. An official Email address would be created within 48 hrs. - 72 hrs. Information regarding the official Email address created would be sent to your current Email address.

Grant An Official E-Mail Id Please.

(Signature of the Head of the Department)

E-mail Requisition Form

Form for Requisition of Official Email Id-

(For Student only)

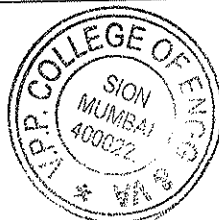|		
First Name	:	
Middle Name	:	
Last Name	:	
Department/ Branch	:	
Roll Number	:	
Current Email address	:	
Mobile Number	:	

Note:

Please spell the names and all other information sought above correctly.

This Email address should be currently used by you.

The filled in form should be submitted after getting duly signed from respective Head of the Department. An official Email address would be created within 48 hrs. - 72 hrs. Information regarding the official Email address created would be sent to your current Email address.

Grant An Official E-Mail Id Please.

(Signature of the Head of the Department)

Wi-Fi Access Requisition Form

Form for Requisition of Wi-Fi Access

(For Faculty & Staff only)

First Name :	
Middle Name :	
Last Name :	
Department/ Branch :	
Current Email address :	
Mobile Number :	

Note:

Please spell the names and all other information sought above correctly.

*This Email address should be currently used by you.

The filled in form should be submitted after getting duly signed from respective Head of the Department.

(Signature of Head of Department)

IT POLICY & GUIDELINES

Wi-Fi Access Requisition Form

Form for Requisition of Wi-Fi Access

(For Students only)

First Name :	
Middle Name :	
Last Name :	
Department/ Branch :	
Roll Number :	
Current Email address :	
Mobile Number :	

Note:

Please spell the names and all other information sought above correctly.

*This Email address should be currently used by you.

The filled in form should be submitted after getting duly signed from respective Head of the Department.

(Signature of Head of Department)