Rayat Shikshan Sanstha's

Karmaveer Bhaurao Patil College, Vashi, Navi Mumbai

[Autonomous]

Policy Document on Information Technology

KARMAVEER BHAURAO PATIL COLLEGE ★ VASHI ★

Policy Document on IT

Document No: KBPCV/IT/PL/01

Prepared By	Reviewed By	Approved By
Dr Manisha Abhyankar Asst. Professor	**Mr Y A Gaikwad** **Asso. Professor**	**Dr Shubhada Nayak** I/C Principal
Date:20/11/2020	Date:19/12/2020	Date:23/12/2020
Governing Body Approval	Date:28/01/2021	Date:28/01/2021
Released By	IQAC	Date:29/01/2021

KARMAVEER BHAURAO PATIL COLLEGE ★ VASHI ★

Table of Contents

Introduction:

The KarmaveerBhaurao Patil College IT Policy and Procedure Manual specifies the policies and procedures for selection and use of IT within the institution which must be followed by all the people of the institution. It also provides guidelines the college will use to administer these policies, with the correct procedure to follow. It also provides expectations aligned with an established mission of providing users with the best resources possible to educate every student. The institution will keep the IT policies updated from time to time and will add new policies or procedures.

Need for IT Policy:

The purpose of IT policy outlines the acceptable use of the network-related systems within the institution. The institution's IT policy exists to maintain, secure, ensure legal and appropriate use of Information technology infrastructure. The policy establishes Institution wide strategies and responsibilities for protecting the CIA i.e. Confidentiality, Integrity and Availability of the information resources that are created, accessed, managed or controlled by institutions. Information resources mentioned in the policy contain data, computers, network devices, intellectual property, documents.

Intranet and Internet services are important resources in educational institutions as active users of network facilities and web based applications have increased over the years. The institution now has 442 computers divided into 14 labs, staff rooms and in offices with proper network connections. The classrooms and seminar halls have ICT facilities. The institution gets its Internet bandwidth from SSV i-ON and SS Broadband having 25 Mbps (leased line) and 100 Mbps broadband connection respectively.

We need to recognize the problems related to uncontrolled surfing by the users like,

- Lengthy or irregular surfing affects the quality of work.
- Heavy downloads that lead to choking of available bandwidth
- Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content. Confidential information being made public.

Network performances suffer in many ways due to large use of Internet like as,

- Internet traffic over Wide Area Network when compared to Local Area Network is a potential bottleneck.
- When free access is given to users i.e critical and non critical users then downloads made by non critical users may clog the traffic which can result in poor Quality of Service and can affect critical users and applications.
- When computer systems are networked, viruses get into the Local Area Network, through Intranet/Internet, spread rapidly to all other computers on the network.

To secure the network, the Integrated Information Committee is taking appropriate action by installing firewalls, access controlling and installing free virus checking softwares. The purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations.

IT policies are classified into,

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- Email Account Use Policy
- Web Site Hosting Policy
- Institution Database Policy

Scope:

This policy applies to students, faculties, consultants, authorized guests and other staff of the institution. This policy applies to all equipment that is owned or leased by Karmaveer Bhaurao Patil College, Vashi including all future purchases.

IT Hardware Purchase and Installation Policy:

Institutional network users need to follow some precautions when computers or its peripherals are being installed so that they may face minimum inconvenience due to interruption of services due to hardware failures. The department head should make an arrangement and make a person responsible for compliance if there are multiple users and none of them are considered as primary users.

- Computers purchased by any Section/Department 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 reinstallation and checking virus related problems also.
- All the computer systems and its resources should strictly be connected to the power supply through UPS. As continuous power supply should be supplied to UPS for battery recharging.
- The connecting network cable should be away from the electrical or electronic equipment as they interfere with the network communication and power supply should not be shared with any electrical or electronic equipment as the power supply is given to computer systems and its resources.
- File and print sharing facilities on the computer over the network should be installed and should be protected with a password with read only access rule.
- Computer systems may be moved from one location to another with prior written intimation to the technicians as they maintain a record of computer identification names and corresponding IP address.
- Procedure for purchasing any Hardware device:
    a. Take three quotations from different companies.
    b. Purchase committee will compare the quotations and decide the best quotation.
    c. Purchase order should be placed after that.
    d. After purchasing, devices should be recorded in the deadstock register of the department.

Software Licensing and Installation Policy:

- Individual users should make sure that respective computer systems have their Operating Systems updated in regard to their service packs/patches, through the Internet for any bug fixes and vulnerabilities in the Operating Systems.
- Wherever possible the institution encourages the user community to go for open source software such as Linux, Open office.
- Computer systems used in the institutions should have antivirus software installed which should be active all time. As the institution has Quick Heal internet security antivirus so individual users should make sure that the respective computer system should have current antivirus protection software installed and maintained.
- Regular backups of their important data should be done by individual users.

Bring your own Device Policy:

- Personal devices should be turned off or set to silent or vibrate mode during meetings and conferences and in other locations where incoming calls may disrupt normal workflow.
- Excessive personal calls, e-mails or text messaging during the workday, regardless of the device used, can interfere with employee productivity and be distracting to others.
- Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft.
- Institution will not be responsible for loss or damage of personal applications.

Information Technology Administration and Security Policy

This policy applies to the entire KBP community of students, employees (both faculty and staff), affiliates, and authorized guests.

KBP requires all individuals to responsibly use information and the information technology employed to collect, process, store, and disseminate it. Acceptance of this policy shall be acknowledged before being allowed access to KBP information technology.

This policy complies with other KBP policies and procedures, particularly policies related to ensuring a harassment-free, discrimination-free, respectful, and professional education/work environment.

Information is data about people, objects, and events, as well as derivations of these data. Information may be text, sounds, and images in electronic form, as well as on paper and other tangible media. Information shall be subject to appropriate and consistent protection, whether in transit, stored in a shared server, cloud storage, workstation, laptop, personal digital device, file cabinet,or wastebasket, copier, fax, database, or other possible locations.

Information created using KBP information technology is an asset of KBP. The information includes confidential and restricted information as well as public information.

Information technology (IT) is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data. KBP information technology includes all hardware, software, and communication networks that KBP owns, leases, or has been assigned control. It also includes non-KBP hardware and software while it is connected to the KBP communication network or to other KBP information technology.

Categories of Responsible Use of Information and Information Technology

Derived from the values held by KBP, there are five categories of responsible use: **Privacy, Lawfulness, Integrity of Information and Information Technology, Improper Use of Information and Information Technology, and Courtesy**.

Privacy

KBP requires faculty, staff and students to ensure the privacy of personal information. Violating or disregarding an individual's right to privacy is a violation of this policy.

KBP technology and information technology user account information, including but not limited to user passwords, may not be transferred to or shared with another without explicit written authorization by the KBP Legal Services in consultation with KBP Vice-Principal.

Lawfulness

KBP requires individuals to obey laws related to information and information technology.

Integrity of Information and Information Technology

KBP requires individuals to ensure the integrity of the information and information technology.

Improper Use of Information and Information Technology Resources

KBP requires individuals to utilize information and information technology resources for business and educational related purposes ONLY.

Courtesy

KBP requires individuals to use information technology in a manner consistent with maintaining optimal professional and respectful work and study environments.

Confidential and Restricted Information

A specific focus of this policy is placed on confidential and restricted information, since KBP values the privacy of the individual. Within the central repositories, each data item or dataset shall be categorized to ensure that sensitive information is limited to those who have a legitimate educational or KBP business-related purpose to use it.

KBP requires individuals to safeguard confidential and restricted information from irresponsible use.

Confidential information, the highest level of sensitivity, is defined as information that could cause substantial damage to or liability for KBP if treated irresponsibly. Restricted information is defined by the need for special safeguards beyond that taken for public information. Public information, the lowest level of sensitivity, may be released according to rules, guidelines, and definitions developed to safeguard the information entrusted to KBP. All information in this policy includes the secure transmission and disposal of information or information technology.

All forms of recorded information and access to that information: written, oral, and visual, regardless of the media, including paper and electronic, shall be safeguarded. The external distribution of confidential and restricted information regardless of the media, including electronic and paper, shall be limited. Safeguarded precautions shall be utilized when providing information in electronic form or other media.

Information and Information Technology Responsible Use Compliance

Employees shall complete and sign a compliance agreement in which he/she agrees to comply with the Information and Information *Technology Responsible Use Policy.*

The compliance agreement shall be available for electronic, as well as handwritten, signature. Other accommodations shall be made for special needs pursuant to state and federal law.

Roles and Responsibilities for Ensuring Responsible Use of Information and Information Technology

The KBP College Principal has ultimate responsibility over the information, including that information intended to reside primarily at the System Office, and for the information technology on which it is stored or processed.

The KBP Legal Official or his/her designee shall:

- Annually review a summary prepared by the KBP Committee responsible for Technology Solutions or his/her designee(s) of the system-and college-level security reports and, if necessary, direct the revision of this policy and associated rules, guidelines, and definitions.
-
- Provide opportunities for the entire KBP community to identify and implement best practices in responsible use of information and information technology and for the information technology administrators to refine their skills in safeguarding information and information technology.

The KBP Official for Technology Solutions shall recommend policies and procedures that ensure:

- That information within central repositories is secure and available.
- That information technology resources shared across KBP College, including the communication network, are secure, available, and appropriately distributed.

Requests for exceptions to this policy shall be submitted for approval to the KBP Principal or his designee the KBP Vice-Principal. All requests shall be submitted in written or electronic form with signature.

In addition, the KBP Legal Official responsible for Technology Solutions shall:

- Annually review and forward to the KBP Vice Principal any suggested modifications to this policy.
- Interpret this policy with advice of the KBP Vice Principal and Cabinet officials.
- Appoint a system-level Information Security Officer within the KBP Office of Technology Solutions to serve as the custodian of all information owned by KBP which is stored centrally, particularly the central database system.

The KBP Principal, KBP Vice Principal primarily responsible for Student Services, KBP Vice Principal and personal responsible for Human Resources and the primarily responsible for Finance shall:

- Assign a System Office designee within their respective areas with direct operational-level responsibility for information management of the records repository who will be responsible for data access, security and integrity, and policy implementation.

The KBP Vice Principal primarily responsible for Institutional Advancement shall:

- Oversee the content within the central repositories with respect to Advancement records and assign a unit designee with direct operational-level responsibility for information management for these records who will be responsible for data access and policy implementation issues.
- Assign a System Office designee within their respective areas with direct operational-level responsibility for information management of the records repository who will be responsible for data access, security and integrity, and policy implementation.

KBP Legal Services shall:

- Review local, state, and federal legislation for potential impact on this policy and its execution as needed.
- Make recommendations on the implementation of this policy and related procedures.
- Advise the KBP leadership on the legality of actions related to irresponsible use, including its investigation.

The system-level Information Security Officer shall:

- Serve as the primary contact for issues related to confidential and restricted information and information technology.
- Recommend rules, guidelines, and definitions for responsible use.
- Ensure that appropriate security controls are enabled and being followed in coordination with each of the unit designees of central repositories, including:
  - Classifying data items within each of the central repositories as "Confidential or Restricted", or "Public" and ensuring security is maintained at an appropriate level based on the classification.
  - Administer policies and procedures for granting and maintaining access privileges for systems containing confidential or restricted information.

The system-level Senior Information Security Analyst shall:

- Serve as a primary resource for forensic analysis as it relates to confidential and restricted information and the support technology devices.
- Implement programs that support rules, guidelines and responsible use.
- Conduct in-depth analysis of potential vulnerabilities as it relates to information security throughout the KBP system.

The college presidents/chief executive officers shall oversee information intended to reside primarily at the college and supervise the information technology located at their college.

The college president/chief executive officer shall:

- Communicate this policy and related procedures regularly to the academic community of the college.
- Identify problem areas to the KBP Vice-President responsible for Technology Solutions, and, if necessary, propose changes to policy, rules, guidelines, and definitions to improve security or reduce irresponsible use, as well as to the system-level Information Security Officer.
- Appoint a college-level Information Security Officer.

The college-level Information Security Officer shall:

- Serve as the custodian of all information and information technology residing primarily at the college.

- Ensure that appropriate security controls are enabled and being followed in coordination with information technology administrators responsible for security administration at the college, including:
    - Classifying data stored locally at the college as "Confidential or Restricted", or "Public" and ensuring security is maintained at an appropriate level based on the classification.
    - Administer policies and procedures for granting and maintaining access privileges for systems containing confidential or restricted information.

The college senior administrator primarily responsible for information technology shall:

- Annually review and forward to the college president any suggested modifications to this policy.

Orientation Training, Ongoing Professional Training and Annual Compliance and Acceptance Review of Responsible Use of Information and Information Technology

All KBP employees shall:

- Complete basic security training; new employees shall complete training before access is granted to information resources.
- Review the requirements for responsible use of information and information technology annually and sign an acknowledgement statement either electronically or manually depending on the mode of delivery. Additional training may be required as best practices evolve.

Some KBP employees may be required to complete advanced training based on their level of access.

Non-compliance Regarding Responsible Use of Information and Information Technology

KBP students, employees, affiliates, and authorized guests shall comply with related laws and KBP policy. Violations shall not be permitted and shall be addressed appropriately by KBP.

Examples of Non-compliance Regarding Responsible Use of Information and Information Technology

Violations of this policy or any attempt to violate this policy constitute irresponsible use. Violations include, but are not limited to:

Privacy

- Viewing or distributing confidential or restricted information without authorization.
- Sharing passwords or acquiring the password of another.
- Failing to protect one's own account from unauthorized use, e.g., leaving a publicly-accessible computer logged on but unattended.
- Transferring confidential or restricted data without authorization to non-KBP devices, including home computers, removable memory devices, and personal digital devices.
- Storing confidential or restricted information on a portable device (such as a laptop, personal digital assistant (PDA), cell phone, or an external storage device) that is subject to loss or theft without authorization and without carrying out proper safeguards.

Lawfulness

- Copying, moving, or capturing licensed software for use on a system for which the software is not licensed or for use by an individual for which the software is not authorized.
- Any unauthorized distribution of copyrighted material using KBP information technology resources is expressly forbidden.
- Using KBP network resources and technology in a peer to peer arrangement or internet downloading for the purpose of obtaining copyrighted materials (such as movies, music and literature) is forbidden in accordance with the Higher Education Opportunity Act.
- Communicating text or images using KBP information technology that is likely to be considered by KBP employees or students to contribute to an offensive or discriminatory work or academic environment.
- Representing the institution using information or information technology without proper authorization.
- Selling or bartering information or access to information technology.
- Disabling security on information technology without proper authorization.
- Concealing one’s own identity in bad faith, i.e., with the intent to deceive.
- Using or allowing use of information technology to access materials likely to be considered pornographic by institution leadership.

Integrity of Information and Information Technology

- Intentionally accessing, using, viewing, distributing, modifying, obscuring, or deleting of data, including information technology administrative data without proper authorization.
- Installing/downloading on KBP information technology any unauthorized software which damages information or restricts the accessibility to the information technology resources (e.g. computer viruses, malware, spyware, etc.).
- Altering a communication of another individual without proper authorization.
- Altering existing information technology without proper authorization.
- Failing to provide the key to encrypted information or passwords to accounts that are needed during an investigation of irresponsible use.
- Intentionally wasting information technology resources, including central processing unit time, storage, network capacity, printing resources, and related supplies.
- Denying access by another individual to information or information technology to which they are authorized.
- Using information technology for non-KBP-related purposes on a routine or extended basis.
- Creating or encouraging communications which may overload the communication network, including unapproved mass emails, “spam”, “chain letters”, and indiscriminate use of “reply to all”.

Courtesy

- Using information technology to advance a personal opinion (except where allowed by free-speech, in which case it must be clearly noted that the opinion does not necessarily reflect the opinion of KBP or where authorized in writing by the KBP Vice President primarily responsible for Institutional Advancement and Communication).
- Making allegations of irresponsible acts by others in bad faith, i.e., with an intent to deceive.

KARMAVEER BHAURAO PATIL COLLEGE ★ VASHI ★

Potential Implications of Non-Compliance Regarding Use of Information and Information Technology

For a student found to have made irresponsible use of information or information technology, the consequences shall be appropriate disciplinary action up to and including, but not limited to, expulsion.

For an employee found to have made irresponsible use of information or information technology, the consequences shall be disciplinary action as appropriate, up to and including, but not limited to, termination.

In addition, KBP may require the individual to reimburse KBP for the computing and personnel charges incurred in the investigation of violation of the rules, including compensation of staff hours and costs for external services provided.

As appropriate, an employee may receive additional training related to the use of information or information technology, be reassigned to another position or other duties in which the employee will not be responsible for using the particular information or information technology, and/or have all or part of their access to information or information technology changed or revoked.

Network (Intranet & Internet) Use Policy:

- The maintenance and support of the network is done by the institutional technical team.
- The problems related to the institutional network should be reported to the technical team.
- The technical assistant should assign an IP address to every computer system which is connected to the institutional network. Proper approach is used to allocate IP addresses to each building i.e. specific range of IP addresses. An IP address allocated to 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.
- A proper server room is present in the institution's Admin building. Server room supplies network connection in the institution buildings. There is a main network cable called Category 6 which shares internet connection. Network switches are present at proper places in buildings.

KARMAVEER BHAURAO PATIL COLLEGE ★ VASHI ★

- A 25 mbps leased line of SSV i-on is present in office and library buildings and 100 mbps broadband connection of SS Broadband is present in other buildings.
- Wifi's are installed in departments.

Email Account Use Policy:

- To increase the efficient distribution of important information to all faculties of institutions, staff, students and other people, it is recommended to use institutional email ids.
- The email facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- When large attachments are to be sent to others, users should make sure that the recipient has an email facility that allows him to receive such large attachments.
- Mailbox user space should be within 80% as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mail.
- Users 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.
- Users should avoid intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

Website Policy:

This policy provides guidelines for the maintenance of all relevant technology issues related to the institutional website.

- Keeping the file up to date will be the responsibility of the Website Committee Chairman and will be responsible for any renewal of items listed in the file.
- All content on the institution website is to be accurate, appropriate and current. This will be the responsibility of the Website Committee Chairman and the members of the Website Committee.

Website File Maintenance

The website file must record the following details:

- List of domain names registered to the institution
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

IT Service Agreements Policy:

- It provides guidelines for all IT service agreements entered into on behalf of the College.
- All College students and employees who use or access Institution's technology equipment and/or services are bound by the conditions of the Procedures.
- The following IT service agreements can be entered into on behalf of the College:
    1. Provision of general IT services
    2. Provision of network hardware and software
    3. Repairs and maintenance of IT equipment
    4. Provision of College software
    5. Provision of mobile phones and relevant plans
    6. Website design, maintenance etc.
- All IT service agreements, obligations and renewals must be recorded in the ICT Service Agreement Register.

Data Loss Prevention Policy

Purpose

- Data Loss Prevention (DLP) encompasses the processes and rules used to detect and prevent the unauthorized transmission or disclosure of confidential information. The purpose of this procedure is to establish a framework of controls for classifying and handling college data based on the data's level of sensitivity, storage location, value, and criticality to the college. The control elements of DLP help to ensure data is utilized in its intended manner.

- Confidential data can reside on or in a variety of mediums (pictures, paper documents, shred bins, physical servers, virtual servers, databases, file servers, personal computers, point-of-sale devices, USB drives and mobile devices) and can move through a variety of methods (human, network, wireless, etc.). The college relies on a variety of DLP strategies and solutions to prevent data loss. The college's DLP strategies and solutions are reevaluated regularly to ensure their relevancy and effectiveness.
- This security procedure applies to all college employees and users of the college's computer systems. Individuals working for institutions affiliated with the college are subject to the same rules when they are using the college's information technology resources or have any means of access to college data that has been classified as confidential or private.

Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the college should that data be disclosed, altered or destroyed without authorization. Classification of data will aid in determining baseline security controls for the protection of the data. All institutional data is classified into one of three sensitivity levels (tiers), or classifications:

Tier1-Confidential Data

Data is classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the college or its affiliates. Unauthorized access to or disclosure of confidential information could constitute an unwarranted invasion of privacy and cause financial loss and damage to the college's reputation and the loss of community confidence. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied.

Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the college who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be requested for an individual and approved by the individual's Vice President, Provost or Executive Director. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data.

Tier 2-Internal/Private Data

Data is classified as Internal/Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the college or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data.

Access to Internal/Private data must be requested for an individual and approved by the individual's Vice President, Provost or Executive Director. Data access granted to individuals must be reviewed and authorized by the Data Owner who is responsible for the data. Access to Internal/Private data may also be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department.

Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the college should this information not be available when needed is typically moderate. Examples of Internal/Private data include official college records such as financial reports, some research data, and budget information.

Tier 3-Public Data

Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the College and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected. The impact on the institution should Level 3 Public data not be available is typically low, (inconvenient but not debilitating).

Data Collections

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student’s name, address and social security number, the data collection should be classified as Confidential even though the student’s name and address may be considered Public information unless specifically marked as Do Not Publish.

Restricted Data

“Restricted data” is a particularly sensitive category of Tier 1-Confidential data. Restricted data is defined as ‘any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transmission’.

Disposal of Technology Equipment policy:

Data Disposal Requirements and Safeguards:

- Paper documents that include confidential or private data and are ready for disposal must be properly shredded. Documents that are awaiting shredding must be stored in a secure location.
- Electronic data files that contain confidential or private data should be deleted and completely removed from the trash, if applicable, as soon as they are no longer necessary.
- Electronic devices that may have contained confidential or private data and are ready for disposal must be drilled or destroyed.
- Departments who wish to dispose of unwanted technology items shall call technical assistants, they will decide whether the device can be reused or not.
- Technical assistants should be notified of any IT equipment which is no longer required, as they can ensure the equipment can be reused or disposed of as appropriate.
- Prior to the disposal of Computer equipment, all personal and sensitive data must be securely destroyed by a method appropriate or if it is necessary then it should be stored properly.

Sr. No	Role	Name	Designation	Signature
1	Prepared By	Dr Manisha Abhyankar	Asst. Professor.	
2	Reviewed By	Mr Y A Gaikwad	Asso. Professor.	
3	Released By	Mr. Bhosale C. D.	IQAC Coordinator	

Approved By:Dr. ShubhadaNayak, I/C Principal

I/C PRINCIPAL
KARMAVEER BHAURAO PATIL COLLEGE
VASHI, NAVI MUMBAI - 400 703.