EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY

Approved by AICTE, New Delhi, Affiliated to VTU, Belagavi
Virgo Nagar, Bengaluru-560049

IT Policy

EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY

IT Policy

Need for IT Policy

- IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, faculty, Staff, Management and visiting Guests and Research Fellowship Members.
- Due to the policy initiative and academic drives, IT resource utilization in the Campus has grown by leaps and bounds during the last decade.

Now, EPCET has network connections to every computer system covering the campus and hostel.

EPCET is getting its Internet bandwidth from BBNL. Total bandwidth availability from BBNL source is 1000 Mbps.

All the faculty, students, staff, departments, authorized visitors/visiting faculty andothers who may be granted permission to use the Institute's information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down bythe institute by any institute member may even result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

- Students: UG, PG, Research
- Employees   (Permanent/ Temporary/ Contractual)
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Resources

- Network Devices wired/ wireless
- Internet Access
- Official Website
- Official Email services
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

- **Policy Objectives: -**

The objectives of the IT policy are as follows:

  o To provide all required IT resources as per the academic programs laid down by AICTE. Also, introduce new IT technologies which will benefit the students and research staff.
  o To effectively have an annual plan of introducing new technologies in-line with the Academia.
  o Create provision for priority up-gradation of the products
  o Create Provision for Annual Maintenance expenses to ensure maximum uptime of the products.
  o Plan and invest for redundancy at all levels.
  o To ensure that the products are updated and catered 24x7 in the campus or as per the policies lay down by the College Management.
  o Leveraging information technology as a tool for the socio-economic development of the Institute.

The Institute has an IT policy covering all major areas like Wi-Fi, cyber security etc. which is updated or amended whenever required as per the need of the institute. Institution tries to have upgradation IT facilities as per the requirement by regulatory norms as well as industry. Institution is regularly upgrading its infrastructure covering Wi-Fi, cyber security, software upgradation, erp system, ICT enabled teaching learning. Formal IT policy has been approved by Internal Quality Assurance Cell (IQAC).

The acceptable use policies are applicable to Employees, Students, Vendors and Visitors. Institutes have framed various policies like Procurement, Installation of Hardware, Network and software. Website Hosting and Database Usage policy has its method and hierarchy which is followed systematically. Certain violations of IT policy by any member may even result in disciplinary action against the offender by institution authorities.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the Institute's administrators, it is recommended to utilize the institute's e-mail services, for formal Institute communication and for academic & 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 Institute communications are official notices from the Institute to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institute 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 https://gmail.com with their User ID

and password. For obtaining the institute's email account, user may contact Computer Center for email account and default password by submitting an application.

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

The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the institute's campus network, or by using the resources provided by the institute to the individual for official use even from outside.

Web Site Hosting Policy

a) Official Pages

Departments, Cells, central facilities may have pages on EPCET's official Web Site

b) Responsibilities for updating Web Pages

Departments, cell, and individuals should contact the respective department website coordinators who are responsible to send updated information time to time about their Web pages to the Website Managing Team.

Institute 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.

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

- **Database Ownership:**

  EPCET 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.

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

1. The institute's data policies do not allow the distribution of data that is identifiable to a person outside the institute.
2. Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal institute purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the institute makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office.
5. Requests for information from any courts, attorneys, etc. are handled by the Office and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for response.
6. Tampering of the database by the department or individual user comes under violation of

IT policy. Tampering includes, but not limited to :
- Modifying/deleting the data items or software components by using illegal access methods.
- Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers.

Such data tampering actions by institute member or outside members will result indisciplinary action against the offender by the institute authorities.

If the matter involves illegal action, law enforcement age