# ICT Policy

## Purpose

This policy defines the policies and procedures to enable the Group to provide a safe and secure information and communication systems environment to support all members in their use of the information and the associated information technology and communications ("ICT") resources. These resources include but are not limited to the Group's computing and network facilities, computer systems and software, data, equipment and processes in its domain and/or control, access to the Internet, electronic mail and messaging, telephony and related services.

This Policy is based on the following essential principles which all Users/Members must adhere to at all times:

a) The ICT resources of the Group are provided to authorize users for the purpose of supporting their learning, teaching, research and administrative activities of the Group.
b) Users who are permitted to access the ICT resources shall do so in a responsible, ethical and lawful manner at all times. Authorised users will be required to comply with Group policies and other laws and **Regulations** as may be applicable from time to time.
c) Confidential and personal information shall be protected and shall not be misused at all times.
d) Group ICT resources shall not be used by users, under any circumstances, to annoy, harass, vilify, threaten, intimidate, offend or humiliate others on the basis of their race, religion, gender or other attribute.
e) All users must inform their Head of Department of any breaches of policy, back up their data regularly and keep their passwords secret and change it regularly to prevent security breaches.
f) The Group may take disciplinary action against users who have contravened the ICT Policy in accordance with the Disciplinary Procedures laid out in the Statutes.

## Coverage

This Policy applies to everyone who accesses Group ICT Resources whether a member of the Group or not, whether on campus or from remote locations and includes, but is not limited to, students, faculty ,full time and part time staff, temporary staff, contractors, consultants ,guests and other permitted users. By accessing or using the Group's ICT resources user agrees to comply with this Policy.



Prof. Mrityunjaya V Latte
PRINCIPAL
EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

### 12.2.1 External Users

All External users who are granted access to the Group's ICT Resources / Systems must adhere to the Group's policies in this regard.

## Definitions

"ICT Resources": For the purpose of this Policy ICT Resources include, but are not limited to allitems of

1) Hardware including personal computers
2) Software
3) Networking equipment, servers, exchanges
4) Transmission lines, networks ,wireless networks
5) Internet connections ,terminals, applications
6) Communication equipment, telephone systems, services and facilities
7) Data and information recorded on all types of electronic media, computer hardware and software, paper, whether Group owned or not, leased, or under license or contract, by the Group, irrespective of where these items may be located and are connected to Group-owned ICT resources.

The use of Group ICT Resources through non-Group (including personally owned) equipmentis also subject to this policy.

Note:

Examples of ICT resources include, but are not limited to:

| | |
|---|---|
| • Central computing facilities | • Financial and other enterprise applications |
| • The Campus Area Network(CAN) | • The ~~Group~~ EPGI WAN |
| • LANs | • Electronic mail |
| • Internet access | • Internet and Intranet Web servers |
| • Webpages | • Public computing facilities |
| • Voice telephony systems | • Wireless network systems |
| • Human resource data | • Student data |
| • Learning and teaching platforms and systems<br>• Mobile Devices | • Electronic Books<br>• Scanners, Printers, Pen drives, CDROMS |



PRINCIPAL
EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

## Communications & Network Infrastructure

The Group's communications infrastructure includes the following:

**Public Network**

This is the network that is fully visible to the outside world and c consists of the web servers which maintain the Group's information on the world wide network.

**Private Network**

This is the Group's-EPGI's private network on which all the Group's operations are conducted.

**Internet**

Web Content of the Group that is made available to users anywhere in the world are available at The Group's official Internet website: ***http://www.eastpoint.ac.in***

## Conditions for Use and Access to IT Resources

1. Use of the Group's ICT Resources is restricted to authorized users and for legitimate Group purposes only. In the case of students this generally means academic coursework and research as approved by a Supervisor. Use by staff members will depend upon the nature of their work.
2. All persons using the ICT Resources shall be responsible to ensure appropriate use of the facilities provided and shall abide by the Codes of Practice defined in this policy.
3. **User Declaration Form:** Users may be required to complete a User Declaration Form before being allowed to access certain ICT Resources.

4. **CODE OF PRACTICE:**
   - i. Users shall respect and protect the privacy of other users at all times;
   - ii. Users shall not use the Group's ICT Resources to collect, use or disclose personal information in ways that breach the Group's the Privacy Policy.
   - iii. Users shall safeguard their data, personal information, account passwords and other authentication codes and confidential information.
   - iv. Users must respect the security mechanisms built into the ICT Resources and to follow the Group's security policies and procedures at all times.
   - v. Users shall at all times comply with all applicable laws governing the use of ICT resources. The Group takes no responsibility for users who breach any **Regulations**.
   - vi. Users shall not use any ICT resources in a manner that constitutes an infringement of copyright. The law permits copying and/or printing only with the permission of the copyright owner, with a few very limited exceptions such as fair use for study

or research purposes (this exception itself is subject to numerous provisos and conditions in the Copyright Act). Accordingly Users shall not download and/or store copyright material, post copyright material to Group websites, transfer copyright material to others or burn copyright material to CDROM so other storage devices using ICT Resources, unless the copyright material is appropriately licensed. Copyright material shall include software, files containing picture images, artistic works, live pictures graphics, computer games, films and music (includingMP3s) and video files.

vii. ICT Resources shall not be used to cause embarrassment or loss of reputation to the Group.

viii. Users must respect the rights of other users and shall comply with the Group's policies on matters relating to religion, sex, race, caste or other attribute.

ix. All internet content made available on the Group's ICT Resources shall comply with the Group's policy on Internet Content.

x. Users shall not use ICT Resources in inappropriate ways, which are likely to corrupt ,damage or destroy data, software or hardware, either belonging to the Group or to anyone else, whether inside or outside the network. They may only delete and alter data as required by their authorized Group activities. ***Note:*** This shall not apply to specially authorized Group computing staff who may be required to secure, remove or delete data and software, and dispose of obsolete or redundant ICT Resources as part of their ICT Resource management duties.

xi. Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorized and competent to do so. All faults or suspected faults shall have to be reported to IT Department of the Group.

xii. ICT Resources shall not be used to distribute unsolicited advertising material from organisations having no connection with the Group or involvement in its activities.

xiii. Users shall not misrepresent themselves or their identity, role or association with the Group in the use of the ICT Resources.

xiv. Users have to identify themselves and not use a false identity. In case where any User of the Group is found to use a fake identity, he/ she shall be subjected to strict disciplinary actions.

xv. Users shall not attempt to gain unauthorized access to any computer service. The use of another person's login, password or any other security device (e.g. Secure ID, digital signature or biometric identification) shall not be permitted. Nor must Users exploit any vulnerability in systems or (except authorised staff when checking security of systems as part of their duties) use any technology designed to locate such vulnerabilities or avoid security systems. Such behaviour if proven would potentially be considered serious misconduct and accordingly may be dealt with under relevant disciplinary provisions. Such instances may be referred to the law enforcement authorities.



Prof. Mrityunjaya V Latte
PRINCIPAL
EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

xvi. Users shall not use ICT Resources for the purposes of subscribing to and accessing fee based services that are for personal use only.

xvii. Users shall not facilitate or permit the use of the Group's ICT Resources by persons not authorised by the Group e.g. Users shall not set up a wireless relay base station from their Group.

xviii. Use of all proprietary software is subject to the terms of the license agreements between the Group and the software owner/licensor.

xix. Personal Information:

All personal information about an individual must not be disclosed without the express consent of the individual concerned.

xx. Confidential Information:

All users have a duty to keep confidential all Group data and information received from other entities and institutions unless it has been approved for publication.

A breach of confidentiality either through negligent or accidental disclosure may result in disciplinary action.

5. Users should recognize that when they cease to be formally associated with the Group (e.g., no longer a student or faculty/employee) their information may be removed from the ICT resources without notice. Users should remove their information or make arrangements for their retention prior to leaving the Group.

**6. Appropriate and Responsible Use:**

Use that is consistent with the maintenance of the highest standards in the pursuit of the Group's mission, the academic, research and other objectives of the Group shall be considered appropriate use; it should be noted that all use that is inconsistent with the above objectives are deemed to be inappropriate use.

Examples of **in appropriate usage** are:

i. Illegal Activities including malicious hacking, pornography, material depicting violence ,inciting others into committing violent acts, injury to human dignity including racial discrimination, incitement to racial hatred, sexual perversion, all types of fraud includingcreditcardfraud,misuseofprivateandconfidentialinformation,unauthoriseduseo fmailservices,damagingothers'reputation,gambling,plagiarismandinfringementsofcopyr ights,Intellectual property rights etc.

ii. Circulating or posting objectionable material of any kind.

iii. Users shall not use any ICT Resource to harass, menace, defame libel, vilify, or discriminate against any other person within or beyond the Group. Users who do so shall be liable even if they aid and abet others who discriminate against, harass or vilify colleagues or any member of the public;



Prof. Mrityunjaya V Latte
PRINCIPAL
EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

iv. Willful wastage of ICT resources is inappropriate use;
v. Users are not permitted to play games whether for competitive or recreational purposes;
vi. Users shall not use any ICT Resources to access, create, store, transmit or distribute pornographic material of any type.
vii. The use of ICT Resources for gambling purposes is forbidden.
viii. Commercial Use: Users may not use ICT Resources for unauthorized profit making or commercial activities.
ix. Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorized and competent to do so .All faults or suspected faults shall have to be reported to IT Department of the Faculty/Group.
x. Users must not attempt to change, alter or delete any of the settings including Network Settings, Control Panel settings, virus scanning software and other applications installed on their machines.

**7. The Group reserves the right to:**

a. Limit, restrict or extend access to Users. The Group also reserves the right to limit permanently or restrict any user's access to the ICT Resources without notice to the user in order to protect the integrity of the ICT resources against unauthorised or improper use;
b. periodically check and monitor the ICT resources and any other rights to protect them;
c. to take any emergency action to safeguard the integrity and security of the ICT resourceswhichrightincludestherighttoterminateusers'access,onlinesessions,changepaswordsanduser names of accounts;
d. Group reserves the right to access or download files by the users of ICT of the Group. Files may only be accessed or downloaded if they are work or study related. In any case, files shall only be downloaded if it is legal to do so and steps have been taken to ensure that the files are free from viruses and other destructive codes;
e. Take disciplinary action if users have been found to be indulging in any illegal or unacceptable use of the ICT Resources including:
    i. Willful physical damage to any of the ICT Resources;
    ii. Improper access to confidential information;
    iii. destruction or deliberate interruption of information or the free usage of other resources;
    iv. disseminating information without appropriate permissions;
    v. engaging in malicious activities including unauthorised access to user accounts and passwords;



Prof. Mrityunjaya V Latte
PRINCIPAL
EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

8. **Reasonable Personal Use**:

Users may be permitted to use the ICT Resources for limited, incidental purposes. Such use must not impose significant additional cost to the Group. Examples of permitted personal use are online banking, travel bookings, browsing for permitted purposes etc.

Reasonable use in the context of the particular circumstances is a matter to be determined by the User's Head of Department or Administrative Head. The Group's decision in this regard shall be final.

9. **Consequences of Breach of Policy**:

Users found to have breached this Policy will be subject to disciplinary action in accordance with the Group's disciplinary procedures and could result in the imposition of fines, recovery of damages and/or costs or even imprisonment. Criminal offences will be reported to the law enforcement authorities.

The Group will not defend or support any user who uses the ICT resources for an unlawful purpose.

Where a user is not a member of the Group and is found to have breached this Policy such users may be subject to action as deemed appropriate by the Group. If the action is criminal in nature it may be reported to the law enforcement officials for action.

**10. Group Course and Other Materials:**

Authorised users of the Group should ensure that all course materials are placed on the Group's servers and not on personal web pages or servers. They are required to observe Group laid down policies and procedures failing which they will be liable to disciplinary action.

**11. Group Liability:**

The Group accepts no liability or responsibility for any loss or damage whether direct or consequential arising from the personal use of the ICT Resources.

### Access for Mobile Computing Devices

Mobile computing devices include hand held devices, other peripheral devices (including printers, disk drives, monitors, keyboards, mice etc.) and associated software.

Mobile computing devices given by the Group to authorized users are the responsibility of the user. These devices must be returned to the Group on demand or when an employee leaves.

Users are required to exercise sufficient care in ensuring that unauthorized persons do not have access to mobile computing devices and to keep information on such devices fully confidential. Passwords should be implemented on such devices to prevent unauthorized access.

Mobile computing devices may be provided access to the Group's network only at designated points or locations.

### Email & Messaging

E mail ids for faculty members, staff and students will be created by the ICT department in a specified format.

The Group owns all copyrights to email correspondence created by members of its staff in relation to their employment duties.

When using the email or messaging systems Users are responsible, at all times:

a) To respect the privacy and personal rights of others;
b) To take all reasonable steps to ensure that no copyrights or IPR are infringed;
c) Not to forward emails containing any personal information;
d) Not to send sexually explicit or other inappropriate material;
e) Not to send SPAM(unsolicited-mails);
f) Not to harass ,threaten or intimidate other persons or users;
g) Not to send forged messages ,forward viruses or other attachments, bulk messages and the like;
h) To ensure that appropriate standards of civility are observed when using email and messaging services, i.e., no angry or threatening messages, offensive, intimidating or humiliating messages may be sent using the ICTR resources;
i) To ensure that care is exercised to refrain from forwarding or copying from any web pages material that is protected by copyright whether it is an audio, video file, music, photographs or text.

### Desktop Environment

The Group will endeavor to implement a standardized desktop environment for all locations to ensure that ICT Department staff can resolve issues efficiently and quickly. The standardized environment will provide users a similar look and feel, uniform access to computer equipment and software applications across the Group support remote access to systems by ICT personnel and users and better maintenance by ICT personnel.

Users must not change or delete any settings that have been made by ICT Department on desktops or other devices. These include Network settings, control panel settings, Icons on the desktop, password settings etc. Users are also required to use passwords and change passwords at regular intervals and to shut down computers etc. using proper procedures.

### Access to the Internet

The ICT Department will provide users with appropriate access to the Internet to perform their functions properly. Users shall abide by the Group's policies in this regard.

a) Users shall use the internet only for approved purposes. Improper usage may result in immediate termination of access.



Prof. Mrityunjaya V Latte
PRINCIPAL
EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

b) Usage may be monitored by ICT Department for any unusual or inappropriate activity. ICT Department's decision in relation to the provision or termination of services to any user shall be final in all matters.

c) Users should respect all copyright laws and other licensing agreements. Failure to do so may result in loss of access privileges and/or penalties.

d) Users will abide by the Acceptable Use Policy of the Group.

e) Users shall not:

- Visit internet sites that contain obscene or other objectionable material;
- Use the internet or email services for illegal purposes, gambling, playing games, commercial purposes.
- Post offensive remarks, comments, indecent material;
- Download any software or other electronic files without using virus protection and/ or filters approved by the Group;
- Use internet access during office hours on non-Group affairs;
- Upload, download or transmit copyrighted material;
- Perform any other inappropriate use prohibited by the ICT Staff.

f) Users who violate any of the above guidelines will be subject to disciplinary action by the Group- as per the policies of EPGI

g) In the case of gross misuse or misconduct access will be terminated immediately and in the case of an employee dismissal procedures will be initiated.

h) All employees and students will be required to sign an undertaking, included in their employment contract, agreeing to abide by the Group's policies and procedures for accessing and using the ICT Resources, email and internet services.

## Security, Privacy and Compliance

**Security & Privacy**

i. Matters of a confidential nature shall only be conveyed or stored in an electronic format when adequate security measures have been taken.

ii. While the Group communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection of confidentiality, privacy or security of any information.

iii. Email and other records stored in ICT Resources may be the subject of a search warrant, discovery order or application under criminal activity. Disclosure outside the Group any personal information, irrespective of its format, shall be considered as breach of information and shall be dealt appropriately.

iv. The Group may collect and receive personal information of Users and others in the course of managing the operation and use of its ICT Resources and that information can be used in connection with efforts to ensure that Users comply with all relevant laws and Group policies.

v. Communications on Group business in any format or media are official records, subject to statutory record keeping requirements and the Group Record keeping

Policy. This shall include emails and received by staff members on any Group related matter. Staff members need to be conscious of the need to preserve official communications in accordance with the relevant Group guidelines on the management of electronic records. Care should be taken before deleting any electronic communication that it is not required to be kept as evidence of a decision, authorization or action.

vi. Sending an email on an official Group matter shall be considered similar to sending a letter on Group letter head. Such email transactions shall have to be handled with the normal courtesy, discretion and formality of all other Group communications. Users shall not write anything in an email that they would not sign of fin a memorandum.

vii. All accounts, data, files, email messages of Users are stored on the ICT Resources of the Group and are normally held private and secure from access by other users. However there may be situations such as repairing, upgrading or restoring servers etc. when properly authorised staff of the Group may be required to:

- Access user accounts;
- Temporarily suspend access to accounts;
- Disconnect computers and/or other ICT resources from the Group's network;

**Access &Physical Control**

i. New Users will be allocated Usernames and Passwords by ICT Department for all systems.

ii. The level of access provided to Users will be based on their need.

iii. Users will be provided with the required User Documentation for all systems maintained by the ICT Department.

iv. Appropriate barriers and controls governing the physical access to, and the maintenance of, the integrity of Group ICT assets shall be deployed commensurate with the risk identified. Such risks include identified natural and environmental hazards.

v. Barriers and controls include, but are not limited to, electronic access control to servers and critical network infrastructure, installations of grillwork surrounding and enclosing video systems, fire suppression, and power management systems. Authentication and authorization functions shall be employed for all users of Group electronic data and information resources. A central authentication database shall be established for all users. Procedures to manage access, authentication and authorization shall be developed to support and manage these activities. Such processes and procedures shall include but shall not be limited to user passwords for network and application access, biometric access mechanism, tokens and electronic key devices.

vi. ***Software and Firmware upgrades:*** All computers, switches, routers and other network-attached devices shall have the most recent approved and released

software and firmware security patches installed as soon as they are generally available.

vii. ***Virus Protection:*** Group approved virus protection software must be installed on all devices on the network. Such software must be regularly updated and scanned for viruses regularly.

viii. ***Malware control:*** Malware is a common feature of globally connected networks. Personnel engaged in the implementation and support of ICT systems shall take all appropriate steps to protect its ICT assets from damage, compromise or loss of confidentiality. For the purposes of this policy, malware is defined as software agents that by their action deny users the maximum capabilities of the ICT systems, compromise the security and confidentiality of Group data and information or destroy or damage ~~Group~~ EPGI ICT assets. Malware include but is not limited to spyware, viruses, worms and spam.

ix. ***Network Interconnections:*** Interconnections among networks are unavoidable in the ordinary course of business. These interconnections are portals for unauthorized access and entry to Group networks and pose significant risk to the security of Group data and information resources. Therefore, all network interconnections shall be guarded, and audited by processes and such perimeter defense and intrusion detection systems, as are appropriate to manage and mitigate these risks.

x. ***Access to Business Critical systems:*** The Group is dependent on several of its major systems for its daily operations. Breaches to their integrity, or their unavailability for any significant period of time, could reduce the service delivery capability or place the institution in disrepute. Such systems may include the Student Administration System, online teaching and learning platforms, the financial management system, the enterprise planning and/or human resource management information system. Notwithstanding the general security safeguards enunciated before, these business-critical systems shall be provided with an elevated level of security. These additional measures shall include, but are not limited to, internal firewalls, secondary access challenges and biometric access controls. When the security requirements are stringent enough, internal isolation of the network segment to which such systems are attached is the final consideration.

## Monitoring

The Group reserves the right to monitor files, data, server logs, websites and e-mails stored on or accessed using the ICT Resources and network of the Group and to access any other device that maybe connected to the Group network including personal computing equipment like laptops. The Group reserves the rights to monitor the use of its ICT resources to ensure compliance with this policy.



Prof. Mrityunjaya V Latte
PRINCIPAL
EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

## Response to Breaches

1. The Group reserves the right to withdraw, restrict or limit any User's access to its ICTR resources if a breach of the seconditions is suspected. Any such suspected breach may also be investigated under other Group laid down processes, and may result in disciplinary action being taken against the offender in accordance with those processes. This may include a request to reimburse costs (e.g. for unreasonable personal use), disciplinary action (including termination of employment/ suspension of candidature) and/ or criminal prosecution.
2. Further the Group reserves the right to remove or restrict access to any material within the Group domain. Such decisions will be communicated to the appropriate supervisor and accountholder.

## Data Backup Procedures

Users should follow the procedures laid down below as far as possible:

### File Naming Conventions

File names should indicate the content of the data within it especially where the files are shared with many users.

### Directory/ Folder Naming Conventions

The users shall be required to comply with the guidelines prescribed in this regard from time to time.

#### Application Directories/Folders

Staff installing applications should use the Default Directories for all applications installed. Where "default directory locations" are not provided the installer must choose the most obvious directory name for installing the application.

#### Backup Procedures

All Users are individually responsible to ensure that their information and data is effectively backed up. The Group does not accept any responsibility for the loss of data or information held on Group ICT Resources or User's personal resources connected to Group ICT resources.

Where several users are accessing/using one computer one person should be nominated with the responsibility of actively monitoring the backup procedures for all information accessed by that group.

Backup logs should be maintained by Users.

All Backups should be appropriately labelled and date indicated clearly. Backups should be stored in a safe, secure and off-site location.



Prof. Mrityunjaya V Latte
PRINCIPAL
EAST POINT COLLEGE OF
ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.

## Hardware &Software Acquisition & Maintenance

Hardware & Software procurements:

i. All requirements of hardware/software should be forwarded to the ICT Department and should be supported with a "Hardware/Software Requisition Form" from the Requisitioning Department together with the justification for the request and duly approved by the relevant authority.
ii. Hardware/Software requests should, as far as possible, conform to the standard configuration, system and applications of software standards laid down by the Group.
iii. The ICT Department may or may not proceed to procure the hardware/software itemrequestedormaymakemodificationstotheconfigurationtoconformtoGroupnorms.
iv. hardware/software purchased should be compatible with the result of the Group' s computer equipment.

**Copyrights:**

Users should be aware of and abide by the Group's policy on copying and using computer software that are protected by copyright and other licenses and laws or contractual agreements with vendors.

**Web Publishing Guidelines:**

EPGI's Publications and outreach committee is responsible for :

- Ensuring that the standards of publication are continuously monitored;
- Resolving all issues relating to the appropriateness of material published on the Group's website.



PRINCIPAL
EAST POINT COLLEGE OF
ENGINEERING & TECHNOLOGY
BANGALORE- 560 049.