I.T.S Engineering College, Greater Noida

IT AND SOCIAL MEDIA POLICY

Social Media Policy

The Social Media policy applies to all kinds of electronic communications, including but is not limited to multi-media, social networking websites, blogs and wikis for both professional and personal use. Consistent with other college policies, internet postings may not disclose any information that is confidential or proprietary to ITSEC-Greater Noida or to any third party that has disclosed information to the college. Internet postings must respect copyright, privacy, fair use, financial disclosure and other applicable laws.

Employees may not claim nor imply that they are speaking on behalf of the college on personal social media accounts. Social media accounts on behalf of the college require approval of college authorities prior to initiation. ITSEC-Greater Noida reserves the right to request certain subjects to be avoided, certain posts to be withdrawn and inappropriate comments to be removed on ITSEC-Greater Noida social media accounts.

Examples of prohibited activity include, but are not limited to:

- Inappropriate posts that may include discriminatory remarks, harassment, or threats of violence
- Posts that could contribute to a hostile work environment on the basis of race, sex, national origin, religion, sexual preference, gender identity or any other status protected by law or by ITSEC-Greater Noida.
- Posts that could be viewed as malicious, obscene, threatening, or intimidating.
- Offensive posts meant to intentionally harm someone's reputation.

IT Policy

The college expects its employees to use college equipments and resources with utmost care and responsibility without compromising on productivity. All employees are expected to use their rationality to ensure that the college equipment and resources are being utilized judiciously. Employees are responsible to ensure that college facilities such as telephone, fax, internet, mail, laptops, data card etc., are not used for personal purposes. This Policy is to ensure that due care is exercised in protecting computing systems and related policy. This policy also governs the use of college information and information systems and seeks to achieve an appropriate balance between information sharing and information protection.

1. DETAILED GUIDELINES FOR COMPUTER, INTERNET/INTRANET BROWSER(S) USAGE

- The system/internet/intranet are college resources and given to employees as business tools to use them for research, professional development and work-related communications.
- Supervisors/Reporting managers should work with employees to determine the appropriateness of using the system/internet/intranet for professional work.
    - ✓ Employees are individually liable for any and all damages incurred as a result of violating college's security policy, copyright, and licensing agreements.
    - ✓ Violation of these policies and/or state and federal laws can lead to disciplinary action, up to and including dismissal and possible criminal prosecution.
- Use of college computers, networks, and internet access is a privilege granted by college authorities and may be revoked at any time for inappropriate conduct including, but not limited to:
    - ✓ Sending chain letters;
    - ✓ Engaging in private or personal business activities;
    - ✓ Misrepresenting oneself or the college;
    - ✓ Engaging in unlawful or malicious activities;
    - ✓ Using abusive, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
    - ✓ Sending, receiving, or accessing pornographic materials;
    - ✓ Becoming involved in partisan politics;
    - ✓ Causing congestion, disruption, disablement, alteration or impairment of college networks or systems;
    - ✓ Infringing in any way on the copyrights or trademark rights of others;
    - ✓ Using recreational games;
    - ✓ Defeating or attempting to defeat security restrictions on college systems and applications; and/or
    - ✓ Downloading of movies, songs and other media for personal purposes.
- Using college automation systems to create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited.
- No employee may use the college 's Internet/Intranet facilities to deliberately propagate any virus, trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the college's networks or systems or those of any other individual or entity.

2. CREATION OF OFFICIAL EMAIL ID

The Teaching, Admin and Technical staff's email creation process begins when new hires are joined into ITSEC-Greater Noida.

Request: On the first day, after completion of new hire joining process, an email will be sent to the Departmental Head by HR, confirming the need of an email id for new hire.

Creation of ID: On receiving the request, the email account is created and an automated email is sent to the Departmental Head containing the new hire's email address, password scheme and any other pertinent information. The email id created will be designation wise and not by the name of employee.

3. OWNERSHIP AND ACCESS OF ELECTRONIC MAIL & DOCUMENTS

- The college owns the rights to all data and files in any computer, network, or other information system used in the college. This includes the right to monitor and right to inspect all computer and e-mail usage.
- Employees must be aware that the electronic mail messages sent and received using college equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by college officials at all times.
- No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the Employee or an appropriate college official.

4. ELECTRONIC MAIL TAMPERING

- Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on other's electronic mail message.

5. RULES FOR ELECTRONIC COMMUNICATIONS

- ***Responsibility:*** Each Employee is responsible for the content of all text, audio or images that they place on or send over the college's e-mail, Intranet or Internet systems.

- ***Professionalism:*** Employees must ensure that their messages are courteous and professional and that the tone and words they use would not cause embarrassment to themselves or the college if the message were made public.

6. DATA/EMAIL HANDLING

Although the college may provide employee with computer, network and phone access, all data stored is, and remains, the property of the college. This includes, but is not limited to, electronic devices, electronic mail, voicemail, instant messages and all files and documents composed, sent, received are remain college property. Hence, all messages/documents need to be required for future reference and needs to be stored properly.

7. DOWNLOADING SOFTWARE

As a policy, employee should never download/transmit any software/applications which could lead to civil or criminal actions against the employee and the college. In case if any employee needs new software/applications, a request duly approved by HOD/Director, needs to be sent to the IT Department for support. IT department will evaluate the request and take necessary steps accordingly.

8. NEW SOFTWARE PURCHASE

- Any new software ***request*** will come from user/department (with approval of Departmental Head) to IT with specification (need etc).
- On receiving the duly approved request, System Manager will ***analyse*** requirement (urgency & cost) and will find the best suitable solution after getting the approval of college authorities.
- After ***approval*** from college authorities, raise the Purchase Order to Vendor, delivery of Purchase Order and receiving with Material Receiving Note (MRN) Document.
- ***Installation & training*** on the software will be given to end user.

9. LOSS / DAMAGE OF COLLEGE ASSET

In the event of a loss / damage of a college Asset, the user, possessing the asset must report the incident to college IT team (along with their Reporting Manager) within 24 hours. The concerned departments, after considering the facts of the matter in question, will assess as to whether the loss / damage is attributed to the negligence / carelessness of the user in question. The principle of natural justice shall be applied and an equal opportunity of being heard shall be given to the user. If the user is found to be guilty of negligence / carelessness, resulting in the loss / damage of the college assets, suitable disciplinary and financial action will be initiated against them.

It is the responsibility of the user to get the documentation done as may be required to file the insurance claim in respect of the lost / damaged college asset (like the Copy of FIR) within the stipulated time limit i.e. 48 hours.

10. IT RELATED PURCHASE POLICY

The aim of this document is to outline the policy and procedures related to the procurement of IT related material, at college.

Purchase Process

- Departmental Heads will put a request to IT Department after taking the approval from Director & college authorities for purchase of IT equipment

and software and it shall be initiated as per purchase process policy available with IT.

11. DATA SECURITY

- Employees are supposed to take approval for all connections to the internet or other private network from IT Department. All computers used in the premises are tracked by IT department.
- Any electronic equipment must be disposed only after ensuring that it may not be accessible by third party.
- Systems must be made available for security update so that latest applications are being updated time to time.

12. DATABASE BACKUP

We expect all employees in ITSEC-Greater Noida to create & maintain appropriate backup of their respective systems.

- ***Backup-*** The saving of files onto External mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- IT Department will ensure timely backup of the server such as daily, weekly at respective locations.
- ***Archive-*** The saving of old or unused files onto External mass storage media for the purpose of releasing on-line storage room
- ***Restore -*** The process of bringing stored data back from the external media and putting it on an online storage system.

13. SECURITY GUIDELINES

a. **Internet Connection Usage**:-

- This specifies how users are allowed to connect to the approved Network and get IT department's approval on all connections to the internet or other private network.
- Requires all connections such as connections by modems or wireless media to a private network or the internet to be approved by the IT department and what is typically required for approval such as the operation of a firewall to protect the connection.
- Also defines how the network will be protected to prevent users from going to malicious web sites.

b. **Asset Control**:-

- This process is meant for the tracking of asset movement from one location to another location. It will define who signs off on the movement of the property.
- In case the system is moved from one location to other, database needs to be updated immediately so that location of all equipments is known. This will help network administrators to protect the network since they will know which user and computer is at what station in the case of a virus infecting the network.
- This also ensures that the data on the computer being moved between secure facilities may be sensitive and must be encrypted during the move.

c. **Mobile Computer Usage (laptop, tab, phone)**:-

- ***Precaution to be taken:*** The authorized employee will accept responsibility for taking reasonable safety precautions with the mobile computer and agree to adhere to college's IT guidelines at all times. The computer user will not be allowed to have administrative rights unless granted special exception by the network administrator.
- ***Configuration:*** All mobile devices owned by the organization or allowed on the organization network must be identified by their MAC address to the IT department before being connected. (Possibly require static IP address).
- The device must meet the computer connection standards and familiar with college IT Guide lines.
- ***Audit of software:*** Devices not owned by the organization are subject to a software audit to be sure no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time.
- ***Access rights*** to the organizational network cannot be transferred to another person even if that person is using an allowed computing device, unless it is approved by the concerned authority.
- ***Firewall:*** Ensure authorized Antivirus/Firewall program with the latest possible updates from time to time. The program shall be configured for real time protection, to retrieve updates daily, and to perform an anti-virus or malware scan at least once per week.
- Additional malware protection software shall be active on the computer in accordance with the anti-virus and malware policy.

d. **Computer Usage Training: -**

Training will be given to all users on the network to make them aware of basic computer threats to protect both their data and the network.

e. **System Update**: -

The systems and applications are checked for security updates by IT department at respective locations and it is the responsibility of IT team to regularly update each system in their respective location. All employees must co-operate/coordinate with IT Team for ensuring timely update of their system.

f. **User Rights**: -

Some of the employees based on the job requirements subject to approval from concerned authority are allowed accessing and controlling of sensitive and internet access to specific sites/programs.

g. **Application Installation/Implementation: -**

IT Department is responsible for installation/implementation of any computer licensed applications on the network to protect both the data used in the application and the rest of the computer network.

h. **Guidelines for the Usage of Mobile Connection/ Landline: -**

- ***Eligibility for Mobile Connection:*** The college, under its corporate connection arrangement, provides Sim card to employees depending upon the role and responsibilities of the employee. Based on this the monthly mobile limit of all individual will be fixed and the employee shall be issued a college owned sim card upon request with/without mobile instrument. Director and college authorities shall be entitled to nominate the employees who shall be provided with the corporate connection. Teaching, Admin and Technical staff members requiring frequent communication will be provided CUG number.
- ***Eligibility for Landline:*** Landline connection will be issued to concerned employee only if required depending upon the role and responsibilities of the employee.
- ***Usage:*** As per college policy it is vital that the mobile connection/ land lines are used as much as possible for all official calls when people are in college.
- ***Issuance of SIM:*** Admin Department will issue the sim card to employee based on the duly filled & approved request in the prescribed format available with HR and Admin department.
- ***Plan type:*** Mobile phone connection will be under CUG in the respective city/location and will be reimbursed only on post-paid connection (official usage).
- ***Bill limit:*** At the end of every billing cycle hard copy bill will be available with HR and the user needs to collect hard copy from HR/ADMIN for review. If any bill exceeds the maximum limits as specified below then the excess amount will be deducted from the subsequent month's salary.

Level	Limit (Post Paid)	Local/STD
Director	(upto Rs. 1500/- per month)	Local & STD
GM/Sr. Manager	(upto Rs.1000/- per month)	Local & STD
Manager / Asstt. Manager	(upto Rs. 500/- per month)	Local & STD
Sr.Exe & Below	(upto Rs. 500/- per month)	Local & STD
Others (Class 4 employees)	(upto Rs. 200/-per month)	Local

- ***Unofficial calls:*** In case of any personal calls, the concerned employee should mark all their personal calls details and accordingly the deduction will be done towards personal calls in the next month salary.
- ***Decorum to be maintained:*** The uses of non-essential features such as caller tunes etc. are not permitted especially to maintain the professional decorum of the college.
- All employees need to keep in mind the professional decorum of the college while choosing the mobile ring tone & keeping its volume to normal level.
- MMS and personal photos on mobile phone instruments are not permitted unless so requested by college authorities.
- Sending of vulgar, malicious and or threatening calls, messages from the phone is strictly forbidden and can result in termination.

Note: The above rules are also applicable when college issues different chips and numbers while roaming domestic and international.