Policy on ICT

General Guidelines:

1. All users should be aware that several network usage issues, violation of which is an offence under national law.
2. The ISME campus-LAN and Internet access resources are meant for official use arising from the academic/research activities and administrative responsibilities of the faculty, staff and students of the College. Use of network resources for personal purposes is discouraged.
3. Users should view the ICT & network resources with a sense of ownership and participation, and should actively help to prevent any misuse. Procedures laid down from time to time regarding the management of ICT & network resources, must be understood and followed meticulously by the user community.
4. The IT Administrator has the right to monitor and scan all information, carried by the network for the purpose of detecting and identifying inappropriate use. As such the privacy of information carried by the network is not guaranteed. IT Administrator is authorized to break open a PC OR disconnect it from the network, if called for.
5. Every user is expected to be aware of the contents of this policy document, and agrees to abide by its provisions. This policy is informed to all the faculty and staff concerned, and all individuals who use ICT & network resources of the College is made aware of this policy.
6. ICT Policy Implementation Committee will be looking into all violations of this policy, and recommend suitable action to the management of the institution.

ICT USAGE POLICY: FAIR / ETHICAL USAGE GUIDELINES

a. All users are expected to make use of the ICT resources accessible to them with sensibility and awareness.

b. The ISME-Intranet and Internet access will not be used for commercial activity, personal advertisement, solicitations, or promotions, such as hosting or providing links of commercial websites or email broadcasts of commercial promotions to the users.

c. Any part/component of the ICT infrastructure of the College shall not be misused for Anti-University, Anti-State or Anti-Government activities. The ICT Policy Implementation Committee is authorized to undertake appropriate measures to ensure maintenance of such discipline and initiate suitable actions for prevention of such undesirable activities.

d. The downloading of audio and video files is to be done strictly for official purposes.

e. Each user must preserve & maintain the confidentiality of the password used by them. No user must try to access the ICT resources using other user's password, either knowingly or otherwise.

f. Access to sites that are banned under law or that are offensive or obscene is prohibited. This is also an offence and will attracts severe punishment.

g. Use of the network to tamper with information on other computers, to deliberately spread harmful/pirated programs, compromise other systems, or to cause damage of any kind, using the intranet/internet is prohibited, and is an offence. The user is liable for any civil losses caused.

h. No equipment/user other than those registered with the College, can be used to connect to the intranet.

CENTRALIZED AUTHENTICATION OF USERS

a. IT Administrator is responsible to devise a mechanism for management of registration and access policy for all users using, for example Active Directory or any other appropriate software. It will provide a GUI based platform for user administration through which user departments can administer their users in the centralized database of users in Active Directory.
b. The IT Administrator is responsible to add/modify the information about the users and their access rights on centralized user database managed by IT Department. The head may designate a staff member, preferably a permanent staff member, to assist him for the user information management of its users on the central user database and inform the IT Department about the same. IT Department under the guidance and support of the ICT Policy Implementation Committee shall provide necessary training to all heads and designated staff members to manage the user information of their respective user department.
c. The user department will update information of its students after finalization of admissions once every year. The modification of user data for teaching, non-teaching staff and any other user is updated immediately by the user department with the change in the user status. Individual user is not responsible for updating of his/her information in the user database.
d. The ICT Policy Implementation Committee will have an authority to override such permissions granted in case of any user

INTERNET & INTRANET APPLICATION SOFTWARE USAGE ONLY BY REGISTERED USERS

a. Registered users will be allowed access to internet facilities and audio and video downloads depending upon their access rights.

International School of Management Excellence
Sy. No. 88, Chembanahalli, Near Dommasandra Circle, Sarjapur Road, Bangalore - 562 125
Corporate Office : CAP-1, Export Promotion Industrial Park, Near ITPL, Whitefield, Bangalore - 560 066
Ph. No. : 91 88806 12345 Email: admin@isme.in Web: www.isme.in

b. Users with selected privileges will be allowed access to Intranet Application Software of the university. For example, only staff of the academic and examination section in the head office and faculty will be given role based access to add/modify/delete relevant data in the Student Management Software.

c. Every Application Software deployed in the College, whether developed in-house or through outsourcing, readymade or cloud based, will have one administrator user designated by the institute. It is the responsibility of the administrator user to manage user access rights. However, non-IT administrators must take guidance and assistance of the Administrative office in resolving technical issues of the software.

d. Access of non-academic websites, download of music/movies and non-academic videos etc. will be restricted for all users.

e. Faster access to e-journals subscribed through National Digital Library & other such projects should be ensured.

ICT SECURITY POLICY:

PHYSICAL SECURITY OF SERVERS, DESKTOP, LAPTOP, PORTABLE DEVICES ETC.

a. The user department where the ICT equipment is installed and used, either temporarily or permanently, is responsible for the physical security of it.
b. It is responsible for allowing the physical access to the ICT resources only to authorized users.
c. Users of a user department can access the network via desktop/laptop computers on the campus network. Users are responsible and accountable for the usage of the systems allocated to them.
d. Users must take adequate & appropriate measures to prevent misuse of network from computer systems that they are responsible for.
e. Individual users as well as User departments should take care of the vulnerability of systems attached to the campus network. In particular, users must apply appropriate service packs, browser updates and antivirus and client security solutions in their MS Windows machines, and necessary upgrades, OS patches, browser updates etc. for other systems.
f. If a user department wishes to set up its own Internet access facility, then it will be done under support and monitoring of the IT Administrator and ensure that deploying such an access facility does not affect the security of the campus network. The user department must completely adhere to the provisions of this ICT Policy for such facility.

USE OF LICENSED SOFTWARE

a. Software programs are covered by copyrights and a license is required for their use.
b. Users / User departments will ensure that they have either an academic, commercial or public license (as in the case of 'free' software) for any software they install on the systems that they are responsible for.
c. Use and exchange of pirated / illegal software over the Campus-Intranet is prohibited. It is the responsibility of the head of the user department to ensure compliance.
d. The downloading and use of software that is not characterized as public domain or 'free' is prohibited.
e. Use of Open Source Software is encouraged to avoid financial burden and legal complications arising out of license management.
f. IT Department should arrange for the training of general purpose Software for all the users

USE OF ANTI-VIRUS & INTERNET/ENDPOINT SECURITY/PROTECTION SOFTWARE

a. The user department is responsible for installation and maintenance of proper Anti-virus or Internet/Endpoint Security/Protection Software or any other security software as prescribed by the ICT infrastructure Management Committee.
b. In case of detection of any issues in the security, the compromised computer/equipment will be disconnected from the Campus-Intranet failing which Computer Centre shall disable the respective network connection.
c. Strict action will be taken by the ICT Policy Implementation Committee against users who deliberately prevent installation of such security software OR disable such software OR prevent them from running.

BACKUP POLICY

a. Every user and user department will manage & maintain backup of data stored on the computers under their control based on its level of criticality. Two months once backup of Restricted Information to be taken depending on its frequency of updates. The backup of server data will be maintained on designated desktop computers by increasing its storage capacity, on regular basis to prevent any data loss.
b. Backup of official data on laptops, external hard drives or any other mobile/removable media to be discouraged.
c. Backup or temporary storage of official data on free public cloud storage facilities like Drobox, Google Drive, OneDrive etc. is unsafe and prohibited.
d. No user/user department should take official data outside the ISME campus without necessary authorization.
e. IT Department will provide Centralized storage facility for all user departments to store backup of their official data only on ISME-intranet. User departments can store ONLY OFFICIAL information using the centralized backup solution.

f. A backup of Critical / Confidential Information will be stored in the local Hard Disk as well as on removable media which may be stored in fire-proof/water-proof safes at different locations to protect critical data from manmade or natural calamities.
g. Periodicity of the backup should be decided based on the level of criticality of information.
h. Information should be classified based on its level of criticality. Users with special privileges should have the accessibility of different levels of critical information.

RESPONSIBILITY

a. User Department will be responsible for security of ICT infrastructure & resources under its control and usage. One permanent staff member shall be designated to supervise and help maintain the ICT security through coordination, guidance and training with the Computer Centre.
b. IT Department will be responsible to provide guidance and training to all user departments in maintaining due security of ICT infrastructure. It is also responsible to assist ICT Policy Implementation Committee in monitoring the implementation of ICT policy on ISME campus.
c. IT Department is responsible to facilitate guidance, support and training to user departments in managing their backup of data.

Nitin Garg
Founder & Director

Rony G Kurien
Dean

Krishnan R
Head Administration

IT Administrator

International School of Management Excellence
Sy. No. 88, Chembanahalli, Near Dommasandra Circle, Sarjapur Road, Bangalore - 562 125
Corporate Office : CAP-1, Export Promotion Industrial Park, Near ITPL, Whitefield, Bangalore - 560 066
Ph. No.: +91 88806 12345 Email: admin@isme.in Web: www.isme.in