Shiksha Mandal's

G. S. COLLEGE OF COMMERCE & ECONOMICS, NAGPUR
(Autonomous)
IT Policy for Staff and Students

Purpose of the IT Policy:

The college has an IT policy for staff and students regular use of computers and other equipment. The purpose of this policy is to establish guidelines for the appropriate and responsible use of equipment, computers, and the internet by staff and students. The students can access computer labs and internet resources in order to ensure efficient and effective utilisation of IT and computer resources while maintaining a secure and productive educational environment.

Scope of the IT Policy:

This policy applies to all students and staff who have access to equipment, computers, and the internet within the educational institution's premises.

General rules to use of Computers, Computer Labs & other IT equipment:

- IT Equipment should be used solely for educational and academic purposes as approved by the institution.
- All IT Equipment should be handled carefully and returned to designated areas after use.
- Personalization or modification of equipment configurations, hardware, or software is strictly prohibited without explicit authorization.
- Computers should be used for educational purposes, including research, assignments, and other activities related to the curriculum.
- Respect the privacy and security of other users by not attempting to access or tamper with their accounts, files, or personal information.
- IT equipment provided by the college should be used solely for official purposes and academic activities.
- Students must adhere to the designated schedule for computer lab access as established by the college.
- Students should follow the lab rules and guidelines provided by the college and follow any specific instructions or restrictions.
- Students must not interfere with or tamper with the hardware, software, or configurations of the computers in the lab.
- To maintain cleanliness and orderliness in the lab.

Internet connectivity and its usage:

- The college is having 300 MBPS internet speed for the staff and student's academic use.

- Internet access is provided to support educational activities only. Students and teachers should use it responsibly and ethically.
- Engaging in activities that are illegal, unethical, or violate the institution's code of conduct, including but not limited to cyberbullying, harassment, or unauthorized sharing of personal information, is strictly prohibited.
- Downloading or accessing unauthorized software, files, or materials that may compromise the security or integrity of the institution's network is strictly prohibited.
- Internet access is provided to students for educational purposes and academic research.
- Users should avoid excessive or unnecessary use of bandwidth that may degrade the overall network performance.
- Users are allowed to connect their personal laptops to the Wi-Fi network, but they are solely responsible for their device's security. Smartphones are not allowed to connect with the college Wi-Fi systems. Access to the Wi-Fi network is granted to registered students, teachers, and office staff members with valid credentials.
- Students must use the internet responsibly, ethically, and in accordance with the institution's acceptable use policies.
- Accessing or distributing inappropriate, illegal, or unauthorized materials, including but not limited to explicit content, hacking tools, or copyrighted material, is strictly prohibited.
- Engaging in cyberbullying, harassment, or any form of unauthorized online behaviour that violates the institution's code of conduct is strictly prohibited.
- Email communication should adhere to professional standards, maintaining confidentiality and refraining from any form of harassment or offensive language.

Use of Computer, Educational Software and Antivirus:

- Computers, software, and applications should be used for official duties, research, administrative tasks, and other work-related activities.
- Unauthorized installation or use of software, including pirated or unlicensed software, is strictly prohibited.
- Accessing or storing inappropriate, illegal, or unauthorized materials, including but not limited to explicit content, hacking tools, or copyrighted material, is strictly prohibited.
- Confidential college data, student information, and other sensitive materials should be handled with the utmost care, ensuring appropriate security measures are in place.
- All the college computers are equipped with legal antivirus, but it is suggested that the users take care of their own data. The college will not be responsible for any data loss.

Security and Privacy:

- Users should maintain the confidentiality and integrity of their accounts and passwords.
- Users must not attempt to bypass security measures, install unauthorized software, or compromise the network's integrity.

- Non-compliance with this policy may result in disciplinary action, including but not limited to temporary or permanent loss of access to computer labs and internet resources, academic penalties, or legal consequences depending on the severity of the violation.
- The college reserves the right to monitor and audit equipment, computer, and internet usage to ensure compliance with this policy and to protect the institution's resources and users.
- Teachers, administrative staff, other college staff and students are responsible for protecting their own accounts, passwords, and personal information while using office computers/college computers/computer labs and internet resources.
- Students must not attempt to bypass security measures, install unauthorized software, or engage in any activity that compromises the security or integrity of the college's network.
- The institution reserves the right to monitor and audit student activities in computer labs.
- Confidential information should not be shared with unauthorized individuals or parties outside the college.
- Any security incidents, breaches, or suspicious activities should be report immediately to the Head of the IT department.

<u>CCTV enabled Campus:</u>

- The college has installed CCTV cameras in all the entry and important points of the college.
- CCTV cameras play a crucial role in enhancing the overall security of a college campus. The presence of visible cameras helps create a sense of surveillance and discourages individuals from engaging in unlawful behaviour.
- CCTV cameras should be strategically placed to provide maximum coverage of high-priority areas, such as entry and exit points, critical infrastructure, parking areas, student gathering spaces, and other locations as deemed necessary.
- Camera positioning and angle should be adjusted to ensure optimal visibility while minimizing the capture of unnecessary or intrusive footage.
- CCTV footage should be considered as sensitive and confidential data. Access to this data should be limited and authorized personnel (HOD IT Department) responsible for security and investigations.
- Access to CCTV footage should be granted on a need-to-know basis and strictly monitored. Proper documentation and logging should be maintained for any access or viewing of the footage.
- Retention periods for CCTV footage should be defined, taking into account legal requirements, incident investigation needs, and storage capacity limitations. Once the retention period expires, the footage should be securely erased or disposed of in accordance with data protection regulations.
- The college should clearly display signage indicating the presence of CCTV cameras in areas where surveillance is conducted.

- CCTV cameras should undergo regular maintenance, including cleaning, testing, and repair, to ensure optimal functionality.

Training and Awareness:

- The college shall provide appropriate training and awareness programs to teachers and office staff members regarding IT policies, responsible use, cybersecurity best practices, and data protection.
- Teachers and office staff members are encouraged to seek guidance from the IT department in case of any concerns or questions related to IT resource usage.

Timely Review of college IT Policy:

- This IT policy for teachers, office staff and students in an autonomous college shall be reviewed periodically to ensure its effectiveness, relevance, and compliance with evolving technological advancements, legal requirements, and institutional needs. Amendments and updates to the policy shall be communicated to all staff members and students as and when required.
- By adhering to this IT policy, teachers, office staff and students contribute to a secure, productive, and responsible IT environment within the autonomous college.

Prof. Pravin Yadao
HOD, IT

G. S. College of Commerce & Economics
NAGPUR

SSKathaley
Dr. S. S. Kathaley
Offg. Principal

Offg. Principal
G. S. College of Commerce
& Economics, Nagpur.