

IT Policy of Government College of Engineering and Ceramic Technology

Introduction:

The Government College of Engineering and Ceramic Technology provides IT resources to support the educational, instructional, research, and administrative activities of the institute and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner. This document establishes specific requirements for the use of all IT resources at the institute. This policy applies to all users of computing resources owned or managed by the institute. Individuals covered by the policy include (but are not limited to) faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, and any other entity which fall under the administration of the institute accessing network services via institute's computing facilities.

The main aspects of the IT policy are to

- i) Develop IT infrastructure and services for laboratories, research, faculty, staff and students on 24 x 7 basis and automation of information management systems
- ii) Regular maintenance and upgradation of IT systems in line with their useful life and their obsolescence.
- iii) Budget provisions to expand ever growing digital systems and services.
- iv) Digitisation of general information and learning resources and access facility through internet and intranet.
- v) Maintenance Firewall and Antivirus for Systems security and Cyber security.
- vi) Maintenance of critical data and necessary backups.
- vii) Maintenance of separate LAN for examinations systems for additional security.
- viii) Use and promote open source software and disposal of e-waste.

Privacy and Personal Rights

- 1) All users of the institute's IT resources are expected to respect the privacy and personal rights of others.
- 2) Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
- 3) While the institute does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

Access to Social Media Sites from Institute's Network

- 1) Use of social networking sites by institute's users is governed by "Framework and Guidelines for use of Social Media for Government Organizations".
- 2) User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.
- 3) User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
- 4) User shall report any suspicious incident as soon as possible to the competent authority.
- 5) User shall always use high security settings on social networking sites.
- 6) User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
- 7) User shall not disclose or use any confidential information obtained in their capacity as an employee of the institute.
- 8) User shall not make any comment or post any material that might otherwise cause damage to institute's reputation.

Intellectual Property:

Material accessible through the institute's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use institute's network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

Software Installation and Licensing Policy

Any computer purchases made by the institute /projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, Institute's IT policy does not allow any pirated /unauthorized software installation on the institute owned computers and the computers connected to the institute campus network. .

Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet.

The institute as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

Antivirus Software and its updating

Computer systems used in the institute should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.

IP Address Allocation

Any computer (PC/Server) that will be connected to the institute network, should have an IP address assigned by the system administrator. Following a systematic approach, the range of IP addresses that will be allocated will be based on Virtual LAN (VLAN) created against each entity or objective. Any device connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP

address unauthorized from any other location. As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies. An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

Use of IT infrastructure

- 1) Each student is to be provided with a PC in the laboratory to carry out his experimental and project related work.
- 2) Few PCs with printing and scanning facility are to be allocated for administrative staff of the institute.
- 3) Every faculty is to be allotted a PC with printing and scanning facility.
- 4) All PCs are to be connected to network having internet facilities.
- 5) All PCs of the institute are to be connected to online/stand-alone UPS.
- 6) All PCs and accessories should be under Annual Maintenance Contract.
- 7) Internet connectivity should be made available to all the VLANs with a provision of 1gbps and above speed.
- 8) Campus wide Wi-Fi connectivity should be made available to all users.
- 9) Access to the network should be proxy based and password protected.
- 10) The internal networks are to be protected by means of application level firewall and a proxy server.
- 11) All laboratories are to be equipped with fire fighting equipment.
- 12) IT infrastructure and its functioning are to be monitored by a committee.