Information Technology is a tool to be used wherever appropriate in order to enhance teaching and learning across the curriculum.

These policies are designed to ensure the effective and responsible use of ICT resources, promote innovation, protect user privacy and security, and foster the growth of the digital economy.

Applicability:

The IT Policy applies to all college faculty, staff and students and all others using the IT resources, whether personally or of college owned, which access, transmitter store various types of related information.

Objectives:

Each user of the College Information Resources must ensure that it is used for promoting the mission of the College towards teaching, learning, research, and administration. In particular, the major objectives of this document are:

- To ensure the integrity, reliability, availability, and superior performance of the College IT Systems
- To ensure that the IT resources protects the official e-identity (allocated by the College) of an individual
- To ensure that all the users of the College are responsible for adhering to the procedures governing the implementation of this Policy document and any other matter incidental to those rules

Security and Integrity:

Personal Use - The College IT resources should not be used for activities violating the basic functionality and mission of the College, except in a purely incidental manner.

The users must refrain from making any unauthorized access of information to promote secure access of Network and Computers.

The competent system administrator may access the information resources for a legitimate purpose.

Firewall - Additional procedures to maintain a secured flow of internet and intranet-based traffic in the campus shall be managed through the use of Unified Threat management (firewall).

Anti-virus and security updates - The regular updation of the anti-virus policy and security updates should be done for the protection of computing resources.

Software Installation and Licensing Policy:

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

- Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or so.
- College 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.
- Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.
- Any software installed should be for activities of the College only.
- Computer systems connected to the internet, used in the College 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.
- 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.

Best Practices

Following best practices shall be adhered to, related to the use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on the College network.

- Firewall should be enabled at all times.
- User shall take prior approval from the IA to connect any access device to the College's network.
- User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy of the application.
- All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less.

- Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.
- User shall report any loss of data or accessories to the IA and competent authority of College.
- User shall obtain authorization from the competent authority before taking any College issued desktop outside the premises of the College.
- Users shall properly shut down the systems before leaving the office/ department.
- Users shall abide by instructions or procedures as directed by the IA from time to time.
- If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the IA for corrective action.
- Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

Discipline for Breach of Policy:

- The college reserves the right to monitor traffic and review all content sent and received on the college systems.
- Breaches of acceptable usage of ICTs will result in disciplinary action.