SAFA | COLLEGE OF ARTS AND SCIENCE

Affiliated to University of Calicut | ISO 9001-2015 Certified | Recognised by UGC 2(f)

IT POLICY

IT POLICY

The purpose of the computing/IT resources at Safa college of Arts and Science is to facilitate the academic, research, and administrative endeavours of the institution. The use of these resources is a privilege that is extended to the members of the institution. The college's IT policy is designed to preserve, secure, and guarantee the proper and lawful use of the IT infrastructure that has been set up on the campus. It also offers guidelines for acceptable and inappropriate usage of the college's IT resources.

OBJECTIVES:

- To regularly oversees, administrate, and manage IT-related campus operations.
- To establish a system for IT-related products and services on the campus, to receive priority upgrades.
- To develop, implement, and support IT and IT-enabled procedures and initiatives that will raise the calibre, efficacy, and accessibility of the college's academic programs.
- To facilitate collaboration between educators and students in the shared digital resources, and to promote development of high-quality e- contents.
- To ensure that the resources are updated and effective for academics.

GUIDELINES:

IT Hardware Installation and Maintenance Guidelines:

- Faculty and the departments can submit IT Hardware requirements based on their academic requirements.
- The departments' requirements and stock availability should be taken into consideration while starting the procurement procedure for IT hardware.
- System administrators handle the installation and periodic maintenance of IT hardware and the same need to be recorded in maintenance register.
- Any movement of IT hardware, either on campus or elsewhere, requires to be documented in the Movement Register.

- The Faculty or the Department is the in charge and accountable for any damage, loss, or theft of the IT Hardware provided to them.
- Every computer and its accessories must be connected to the power source using a UPS.
- Annual Maintenance Contract should be maintained by the system administrator.

Software Installation and Licensing Guidelines

- Only approved/authorised/Licensed software should be installed on college computers according to IT regulation. The Department or the Individual shall be held personally liable by the College for any violations.
- Backups of data should be made on a regular basis by system administrators and stored in external hard drives.
- Academic and administrative software should comply with ISO standards.
- Prior authorization from the system administrator is required for the installation and updates of software on smart TVs.

Network (Intranet & Internet) Use Guidelines

- An IP address must be provided by the system administrators to any PC or server that will be linked to the college network.
- It is highly forbidden for staff members or students to change the IP address of any computer.
- Configuration of a network will be done by system administrators only.
- Internet and Wi-Fi facilities should be used for academic and administrative purpose only.

Web Site and College Database Use Guidelines

- Stakeholders should use the college website to get administrative and academic information.

- The official website for the college should be updated regularly by the administrator. The contents for the official social media accounts should upload after prior approval of the principal.
- The system administrator must take the necessary precautions to ensure the security of the data hosted on the website.
- The College is the owner of all institutional data created within the College.
- The databases maintained by the College administration under the College's e - Governance must be protected.
- The sharing of data with an individual outside the College is prohibited by the College's data regulations.

Requests for information from any courts, attorneys, etc. are handled by the Office of the College. Departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the principal.

Cyber Security Measures

- Users must comply with all cyber security measures implemented by the system administrator, including regular password changes and two factor authentication.
- Reporting of any suspicious activities, phishing attempts, or security concerns is mandatory.