INDIAN ACADEMY
Degree College - Autonomous

Information Technology Policy and Guidelines

1. Introduction

The IT policy streamlines both academic and administrative operations of Indian Academy Degree College – Autonomous (IADC-A). This policy is applicable to staff and students using the IT resources owned by the institution. The consequence of inappropriate usage of the IT facilities could be unwanted risks and a liability to the institution. Therefore, it is expected that these resources are used for institution related activities in an ethical and lawful manner.

2. Scope

The IT policy administers the usage of IT resources from an end user's perspective. This policy applies to all staff and students using IT resources.

3. Policy Objectives

- To provide all necessary IT facilities as per the academic programmes offered by the institution
- The policy ensures proper utilization of all IT resources
- It prevents misuse of IT resources
- To periodically introduce recent trends in IT that will benefit the staff and student community
- To create facilities for maintenance and upgradation of the products and processes

4. Privacy

i. IADC-A reserves the right to access and review transmitted information with the approval of the Principal.

ii. The staff and students are expected to respect the privacy and personal rights of others and refrain themselves from copying data / programs / e-mail content / other files without authorization and approval of the Principal.

5. Intellectual Property

Content accessible and available in the IADC-A network and other resources are subject to protection under Privacy, publicity, personal rights and Intellectual Property Rights. Staff and students shall not use the Institution's network and resources in any manner that would infringe or violate any such rights.

6. Review

Technical enhancements in the policy shall be made by the technical team with the approval of the Principal.

7. Sharing of Data

Staff and students shall not share confidential information including account(s) and password(s) or similar information which is used for identification and authorization.

8. Roles and Responsibilities

i. IADC-A shall implement necessary controls to ensure user compliance with the IT policy.

ii. Staff and students shall use IT resources for academic and administrative purposes only.

iii. The staff and students are expected to adhere to all applicable laws.

iv. Staff and students shall not install any network / security device on the network without consultation with the Technical Team.

v. All staff and students are expected to respect the reputation of the institution in activities related to use of ICT communications within and outside the institution.

9. E-mail Access

As a step towards effective distribution of information to staff and students, it is recommended that authorized e-mail services shall only be used for official correspondence. All formal communications for academic and administrative purposes shall be through the official e-mail addresses. In order to receive official communications, e-mail addresses are to be kept active by using the same regularly.

10. Security Incident Management Process

i. The college reserves the right to deactivate or remove any software application or network if it is a threat that can lead to a compromised system.
ii. Any security incident must be brought to the immediate notice of the Principal.

11. Deactivation

In case of any security threat to the systems or network at IADC-A, the resources being used may be immediately deactivated by the technical team and the Principal shall be kept informed.

12. IT Hardware Installation Policy

When a connection is established with the network, the connecting cable has to be kept away from the electrical or electronic equipment as it interferes with network communication. No electrical or electronic equipment shall be shared with the power supply of connected computers and peripherals.

File sharing and print facilities on the computers over the network must be installed only if it is an undeniable necessity. Files shared over the network, should be password protected with read-only access rights.

The computers and peripherals must be connected to electrical points only through the UPS and the power supply to the UPS should always be on. UPS systems are to be connected to the electrical points with properly laid electrical wiring.