

A.S.D.GOVERNMENT DEGREE COLLEGE FOR WOMEN

An Autonomous Institution, Affiliated to Adikavi Nannaya University

INFORMATION TECHNOLOGY POLICY

1. Introduction

A.S.D. Government Degree College for Women(A) is committed to leveraging Information Technology (IT) to enhance educational and administrative processes. This IT Policy outlines the guidelines and standards for the use, management, and security of IT resources at the college. The aim is to ensure the effective, efficient, and secure use of technology to support the college's academic and operational goals.

2. Purpose

The purpose of this IT Policy is to establish clear guidelines for the use of IT resources, protect the integrity, confidentiality, and availability of the college's IT infrastructure, ensure compliance with legal and regulatory requirements, and promote a safe and secure IT environment for all users.

3. Scope

This policy applies to all students, faculty, staff, and any other individuals who use the IT resources of the College. IT resources include hardware, software, networks, and data.

4. Objectives

The primary OBJECTIVE of this Information Technology Policy are to ensure the effective and efficient utilization of IT resources, safeguard the integrity, confidentiality, and availability of the college's IT infrastructure, promote a secure and reliable IT environment, and ensure compliance with all relevant legal and regulatory requirements. By establishing clear guidelines and responsibilities, this policy aims to support the academic and administrative functions of the college, protect sensitive data, prevent unauthorized access and activities, and foster a culture of responsible and ethical use of technology among all users.

5. Annotation

IT Infrastructure IT infrastructure refers to the composite hardware, software, network resources, and services required for the existence, operation, and management of the college's IT environment. This includes physical devices such as computers, servers, and networking equipment, software applications and services, data storage systems, and all networking components that facilitate connectivity and communication. The IT infrastructure supports the delivery of information technology services and solutions necessary for the academic and administrative functions of the college.

User A user is any individual who utilizes the IT resources of the Government Degree College. This includes students, faculty, staff, and any other individuals who have been granted access to the college's IT systems. Users are responsible for adhering to the IT policies and guidelines set forth by the college and for ensuring their activities on the college's IT systems are lawful and appropriate.

User Account A user account refers to access/permission granted to an individual user, which allows them access to the college's IT resources.

6. Acceptable Use

All users must use IT resources for educational, research, and administrative purposes only, respect the intellectual property rights of others, avoid any activity that could harm the IT resources or disrupt the operations of the college, refrain from using IT resources for unauthorized commercial activities or personal gain, and ensure that personal use of IT resources does not interfere with the performance of their duties or the performance of the IT resources.

7. User Responsibilities

Users are responsible for protecting their passwords and accounts, ensuring that their use of IT resources complies with this policy and all applicable laws, keeping their personal devices used for college work secure and updated, and refraining from unauthorized access to other users' accounts or IT resources.

Students: Students must use IT resources primarily for educational purposes, comply with IT policies, report any security incidents, and respect the privacy and security of others.

Faculty: Faculty members must ensure the use of IT resources in their teaching and research activities complies with this policy, protect the privacy of student information, and report any IT issues or security incidents.

Staff: Administrative staff must use IT resources to support the operational functions of the college, ensure data privacy and security in their respective domains, and promptly report any IT issues or security breaches.

8. Policy Statements

Data Security and Privacy

Sensitive data must be encrypted both in transit and at rest. Access to sensitive data is restricted to authorized personnel only. Users must adhere to data protection regulations, including those pertaining to the privacy of student and staff information. Regular backups of critical data must be performed and securely stored.

Software Management

Only licensed and approved software may be installed on college-owned devices. Software must be regularly updated to protect against vulnerabilities. Unauthorized copying or distribution of software is prohibited.

Internet and Email Use

Internet access is provided to support the educational and administrative functions of the college. Users must not access, download, or distribute illegal or inappropriate content. Email accounts provided by the college are for official use only. Users must be cautious of phishing attempts and report suspicious emails to the IT department.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- i. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- ii. Using the facility for illegal/commercial purposes is a direct violation of the College's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- iii. While sending large attachments to others, user should make sure that the recipient has email facility that allows him/her to receive such large attachments.
- iv. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- v. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
- vi. Impersonating email account of others will be taken as a serious offence under the College IT security policy.
- vii. It is ultimately each individual's responsibility to keep their e-mail account free from violations of College's email usage policy.

Privacy

The college respects the privacy of all users and expects users to respect the privacy and security of others. Personal information must be handled in accordance with data protection regulations.


9. Compliance and Enforcement

Compliance with this policy is mandatory. Violations of this policy may result in disciplinary action, including but not limited to suspension of IT privileges, disciplinary review, or legal action.

10. Policy Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in technology or regulatory requirements. Feedback from users will be considered in the review process.

This Information Technology Policy ensures that all members of the College community use IT resources responsibly, securely, and in alignment with the college's goals and legal requirements.


PRINCIPAL
A.S.D.GOV'T.DEGREE COLLEGE (M)
AUTONOMOUS
KAKINADA