DANTULURI NARAYANA RAJU COLLEGE
(Autonomous)
BHIMAVARAM, W.G.DIST, ANDHRA PRADESH, INDIA, PIN- 534202.
(Accredited at 'B$^{++}$' level by NAAC)
(Affiliated to Adikavi Nannaya University, Rajamahendravaram)

# IT POLICY

of

## DANTULURI NARAYANA RAJU COLLEGE (D.N.R.)
## (Autonomous)
## BHIMAVARAM – 534 202

# IT POLICY

**Preamble:**

Danthuluri Narayana Raju College (Autonomous) is committed to the responsible usage of its information technology (IT) resources. This policy outlines the principles and guidelines governing the use of all IT facilities provided by the College, whether centrally managed or department-specific. All members of the College community, including faculty, staff, students, and others using College IT resources, are expected to be familiar with and adhere to this policy.

## Applicability

This IT Policy applies to all faculty, staff, students, and any other individuals using the College's IT resources, whether personal or College-owned, that access, transmit, or store information related to the College.

## Objectives

The primary objectives of this policy are:

- To ensure the integrity, reliability, availability, and superior performance of the College’s IT systems.
- To protect the official e-identity (allocated by the College) of individuals.
- To establish procedures for the implementation of this policy and related rules, ensuring that all users comply.

## Need for IT Policy

- To maintain, secure, and ensure the legal and appropriate use of the College’s IT infrastructure.
- To set strategies and responsibilities for protecting the confidentiality, integrity, and availability of information assets managed by the College.
- To address issues related to internet bandwidth limitations, infrastructure constraints, financial limitations, and technical manpower for network management.

## IT Usage and Prohibitions

- **Authorized Use**: IT resources should be used to support the College's mission of teaching, learning, research, and administration. This includes using campus collaboration systems, internet resources, official websites, Management Information Systems (MIS), ERP solutions, Learning Management Systems (LMS), remote login facilities, and e-Library resources.
- **Compliance**: Users must comply with College policies and legal obligations, including respecting licenses and contracts.
- **Awareness Programs**: The College will provide awareness programs to familiarize users with effective IT resource usage.
- **Prohibited Use**: Users must not send, view, or download materials that are fraudulent, harassing, obscene, threatening, or otherwise violate applicable laws or College policies. Activities that contribute to a hostile academic or work environment are prohibited.
- **Copyrights and Licenses**: Users must respect copyright laws and licenses. Unlawful file sharing is prohibited.
- **Social Media**: Users must follow College rules regarding social networking sites, mailing lists, newsrooms, chat rooms, and blogs.
- **Commercial Use**: IT resources must not be used for commercial purposes, advertisements, solicitations, or other promotional activities unless explicitly permitted by College rules

## Security and Integrity

- **Personal Use**: IT resources should not be used for activities that violate the College's mission, except in an incidental manner.
- **Unauthorized Access**: Users must refrain from unauthorized access to information. The system administrator may access information resources for legitimate purposes.
- **Firewall**: A Unified Threat Management (UTM) firewall will manage and secure internet and intranet traffic.

- **Anti-virus and Security Updates**: Regular updates of anti-virus software and security patches are required to protect computing resources.

## IT Asset Management

- **Asset Management**: Procedures for managing hardware and software assets, including purchasing, deployment, maintenance, utilization, energy audits, and disposal, will be established.
- **Copying and Distribution**: The College will ensure compliance with copyright and licensing laws regarding the copying and distribution of software.
- **Risk Management**: Procedures will be established for identifying, minimizing, and monitoring risks. This includes timely data backup, replication, restoration, power backups, audit policies, and alternative internet connectivity.

## Operating Aspects

- **Governance**: The implementation of this policy will be overseen in accordance with the College’s governance structure, ensuring fair and consistent application.

## Review and Monitoring:

This IT Policy is dynamic and will be reviewed and updated regularly to reflect changing technology, user needs, and operational procedures. All users are expected to stay informed about any modifications to the policy.

Review of the Policy Document shall be done by a Committee chaired by Principal and Chairman IQAC of the college. The Other members of the Committee shall comprise website in-charge , Technical committee , Heads of the Departments and other members nominated by IQAC.