Department of Higher Education

Govt.of Andhra Pradesh

SKVT GOVERNMENT DEGREE COLLEGE:: RAJAMAHENDRAVARAM

e-GOVERNANCE and

DIGITAL RECORDS MANAGEMENT POLICY

2026-27

A] e-GOVERNANCE POLICY -2026

SKVT Government Degree College, Rajamahendravaram, with a view to improve quality educational services delivery, improved transparency in administration, to enhance efficiency, and digital integration across all academic and administrative functions, has adopted a comprehensive e-Governance Policy. The policy covers admissions, examinations, finance, library, ICT infrastructure, alumni, and feedback systems, aligning with national digital governance standards.

Key Highlights of SKVT E-Governance Policy

🎯 **Objectives**

- Transparency & Accountability in administration
- Efficiency through automation and digitization
- Real-time access to institutional data
- Cybersecurity & Data Privacy compliance
- Global visibility of the institution

🏛️ Scope of Implementation

- Academics: e-plans – Semester Curricular Plan
- **Administration:** Centralized information system for policies and decisions
- **Student Admissions**: Online portals, digitized records, merit lists
- **Examination & Evaluation**: Automated exam cell, digital results, secure evaluation
- **Library Management**: E-library, digitized catalogs, resource tracking
- **Finance & Accounts**: Digital records, automated reporting, secure storage
- **ICT Infrastructure**: Cloud platforms, AI-enabled analytics, automation tools
- **Alumni Management**: Online alumni portal, networking, career guidance
- **Feedback System**: Online feedback from students, faculty, stakeholders
- **Research & Innovation**: Digital project tracking, publications, patents

🌐 Digital Platforms

- **E-Office Platform**: Information sharing through e-office module both internally and externally from 15.9.2026.
- **Website & Social Media**: Updated in real-time with notices, achievements, and academic information
- **ERP System**: Integrated modules for student records, HR, finance, courses, and evaluations
- **Communication Channels**: Email, messaging apps, and dedicated platforms for stakeholder interaction

📊 Benefits

- Faster service delivery
- Reduced paperwork → Greener campus

- Enhanced stakeholder engagement
- Improved accountability and decision-making
- Streamlined academic and administrative processes

⚠️ Challenges & Safeguards

- Digital Divide: Ensuring access for rural students
- Cybersecurity Threats: Strengthened protocols for safe data management
- Resistance to Change: Training and awareness programs for staff
- Infrastructure Limitations: Continuous upgrades to ICT facilities

📌 Conclusion

The SKVT Government Degree College e-Governance Policy is designed to transform the institution into a digitally empowered campus. By integrating ICT tools, ERP systems, and secure communication platforms, the college ensures SMART Governance (Simple, Moral, Accountable, Responsive, Transparent) for students, faculty, and stakeholders.

B] DIGITAL RECORDS MANAGEMENT POLICY-2026

1. Preamble

SKVZT Government Degree College, Rajamahendravaram recognizes the increasing importance of electronic records in academic, administrative, financial and institutional activities. The College shall maintain digital records in a systematic, secure, accessible and legally compliant manner.

This policy provides guidelines for the **creation, classification, storage, preservation, access, security, retention, backup and disposal of digital records** generated or received by the College.

2. Legal Basis

The policy shall be implemented with reference to applicable laws, rules and government instructions, including:

- **Information Technology Act, 2000**, particularly provisions relating to electronic records and electronic signatures.
- Applicable Government of India and Government of Andhra Pradesh rules concerning electronic records and e-governance.
- Applicable records-retention and archival requirements prescribed by competent authorities.
- Institutional policies relating to confidentiality, cybersecurity and data protection.

Note: The IT Act provides legal recognition to electronic records; it does not by itself prescribe the complete retention period for every type of college record. Retention periods should therefore follow the applicable departmental/government record-retention schedules.

3. Definition of Digital Record

For this policy, a **digital record** means information created, received, generated, maintained, transmitted or stored in electronic form and capable of being retrieved and used subsequently.

Examples include:

- PDF and Word documents
- E-mails
- Electronic proceedings and minutes
- Student databases
- Examination records
- Financial records
- Scanned documents
- Digital photographs and videos
- Online applications and forms
- E-office files
- Library databases
- Website records
- Electronic correspondence

4. Objectives

The objectives of the policy are to:

1. Ensure systematic management of digital records.
2. Maintain the authenticity, integrity and reliability of records.
3. Facilitate quick retrieval and use of institutional information.
4. Reduce dependence on paper records wherever legally and administratively permissible.
5. Protect confidential and sensitive institutional information.
6. Prevent accidental loss, unauthorized alteration or destruction of records.
7. Establish appropriate backup and disaster-recovery mechanisms.
8. Ensure compliance with applicable laws and government instructions.
9. Support transparency, accountability and good governance.
10. Preserve important institutional records for future reference.

5. Scope

The policy applies to digital records created, received or maintained by:

- Principal's Office
- Academic departments
- Administrative office
- Examination section
- Accounts section
- IQAC
- Library
- NSS/NCC and other cells
- Sports and Games section
- Student-support services
- Committees and statutory bodies
- Any other unit or cell of the College

6. Classification of Digital Records

Digital records may be classified as follows:

A. Academic Records

- Admission records
- Attendance
- Internal assessment
- Examination records
- Results
- Academic plans
- Teaching-learning documentation

B. Administrative Records

- Office orders
- Proceedings
- Circulars
- Meeting minutes
- Correspondence
- Staff-related records

C. Financial Records

- Bills
- Vouchers
- Receipts
- Budget records
- Audit documents
- Procurement records

D. Institutional Quality Records

- IQAC records
- AQAR documentation
- Accreditation-related evidence
- Feedback reports
- Academic and administrative audit reports

E. Library Records

- Accession records
- Membership records
- Circulation data
- Digital-resource records

F. Multimedia Records

- Photographs
- Videos
- Audio recordings
- Event documentation

7. Creation and Naming of Digital Records

All official digital records should:

- Have meaningful file names.
- Include appropriate dates or reference numbers.
- Be stored in the designated institutional location.
- Use standard file formats wherever practicable.
- Avoid unnecessary duplication.
- Clearly identify the responsible section or department.

Suggested format:

Department_RecordType_Year_ReferenceNo

Example:

IQAC_AQAR_2025-26_01.pdf

8. Storage and Organization

The College shall establish appropriate institutional digital storage arrangements.

Records should be organized according to:

College → Section → Record Category → Academic/Financial Year → Record

Important records should not be maintained exclusively on an individual employee's personal computer or personal cloud account.

9. Backup Policy

The College shall maintain appropriate backup arrangements for important digital records.

Recommended approach

- **Primary copy:** Institutional computer/server/cloud storage
- **Backup copy:** Separate backup storage
- **Important archival copy:** Secure offline or otherwise protected storage

Backups should be performed at appropriate intervals based on the importance and frequency of changes to the records.

Backup restoration should also be periodically tested.

10. Security of Digital Records

The College shall take reasonable measures to protect digital records from:

- Unauthorized access
- Accidental deletion
- Malware and ransomware
- Unauthorized modification
- Data corruption
- Theft or loss of storage devices

Security measures may include:

- Strong passwords
- Role-based access
- Antivirus/endpoint protection
- Regular software updates
- Access controls
- Encryption where appropriate
- Secure backups
- Periodic security reviews

11. Access Control

Access to digital records shall be based on **official responsibility and need-to-know principles**.

Record category	Suggested access
Public notices	General/public access
Academic records	Authorized academic staff
Student personal records	Authorized personnel
Financial records	Principal/Accounts/authorized officers
Service records	Authorized administrative personnel
Confidential committee records	Authorized members/officials
Examination confidential material	Strictly restricted access

12. Authenticity and Integrity

The College shall take measures to ensure that official digital records remain:

- **Authentic** – identifiable as the record created or received by the concerned authority.
- **Reliable** – accurately representing the transaction or activity.

- **Integral** – protected against unauthorized alteration.
- **Usable** – capable of being located, retrieved and understood.

Where legally or administratively required, appropriate **electronic/digital signatures, access logs, timestamps or other authentication mechanisms** may be used.

13. E-mail as an Official Record

Official e-mails that document decisions, approvals, instructions, transactions or important correspondence should be preserved when they constitute institutional records.

Important e-mails should not be deleted merely because they are old, if they are subject to applicable retention requirements.

14. Scanning and Digitization

When physical records are digitized:

1. The scanned copy should be complete and legible.
2. Appropriate file naming should be used.
3. The source record and digitized record should be appropriately cross-referenced.
4. Important documents should be checked for completeness.
5. Digitized records should be stored securely.
6. Original physical records should be retained or disposed of only in accordance with applicable rules.

15. Retention and Preservation

The College shall establish **record-specific retention periods** based on applicable government/departmental record-retention schedules.

Records may be categorized as:

- Temporary records
- Routine records
- Important administrative records
- Permanent/archival records

Examples of records that may require long-term preservation include institutional proceedings, important policy documents, accreditation records, historical photographs and significant institutional reports, subject to applicable rules.

16. Disposal of Digital Records

Digital records shall not be deleted merely because they are no longer frequently used.

Before disposal, the responsible authority should verify:

- Whether the retention period has expired.
- Whether the record is required for audit.
- Whether it is subject to legal proceedings.
- Whether it has historical/archival value.
- Whether any government instruction requires continued preservation.

Deletion of records should be authorized and, where appropriate, documented.

17. Disaster Recovery

The College should maintain a basic **Digital Records Disaster Recovery Plan** covering:

- Hardware failure
- Cyberattack
- Malware/ransomware
- Accidental deletion
- Fire, flood or other physical disaster
- Loss or corruption of storage media

Critical records should be capable of being restored from reliable backups.

18. Responsibilities

Principal

- Overall authority for implementation of the policy.
- Approves major procedures and access arrangements.
- Ensures compliance with applicable government requirements.

Record Custodian/Section Head

- Maintains records of the concerned section.
- Ensures proper classification, storage and retention.
- Controls authorized access.

IT/System Administrator

- Maintains digital infrastructure.
- Implements backup and security measures.
- Assists in recovery of lost/corrupted records.
- Maintains appropriate technical safeguards.

IQAC

- May monitor digital documentation relating to quality initiatives, accreditation and institutional performance.
- Facilitates systematic maintenance of documentary evidence required for quality assurance.

All Employees

- Protect official digital records.
- Follow access and security procedures.
- Avoid unauthorized copying, alteration or deletion.
- Report loss, corruption or suspected unauthorized access promptly.

19. Digital Records Register

The College should maintain a **Digital Records Register** containing at least:

Sl. No.	Record Category	Section	File/Record Description	Year	Storage Location	Retention Period	Custodian	Backup

This register can serve as important evidence of systematic institutional record management.

20. Review of the Policy

The policy should be reviewed periodically, preferably **once every two years** or whenever there are significant changes in:

- Information technology
- Government regulations
- Institutional systems
- Cybersecurity requirements
- Records-management practices

21. Conclusion

Effective digital records management will help SKVZT Government Degree College maintain **transparency, accountability, institutional memory, operational efficiency and secure access to information**. The College shall progressively strengthen its digital record-keeping practices while ensuring compliance with applicable laws, government rules and institutional requirements.

Suggested Institutional Resolution

"Resolved that the Digital Records Management Policy of SKVT Government Degree College, Rajamahendravaram be adopted with effect from 15.9.2026 and that all departments, sections, cells and committees of the College shall maintain digital records in accordance with this policy and applicable Government rules."



PRINCIPAL