INFORMATION TECHNOLOGY (IT) POLICY– 2026

Sharnbasva University, Kalaburagi

Table of Contents

1. Preamble

Sharnbasva University ("the University") relies on Information Technology (IT) systems, networks, applications and data as core infrastructure supporting teaching, learning, research, administration and outreach. This IT Policy ("the Policy") establishes the principles, rules and responsibilities that govern the acquisition, deployment, use, security and management of all IT resources owned, leased, licensed or operated by or on behalf of the University.

This Policy applies alongside, and does not override, applicable laws of India, including but not limited to the Information Technology Act, 2000 (as amended), the Digital Personal Data Protection Act, 2023, UGC/AICTE regulations, and any University Statutes, Ordinances or Regulations in force.

2. Objectives

1. To ensure the confidentiality, integrity and availability of University IT resources and data.
2. To provide a secure, reliable and efficient IT environment for academic, research and administrative activities.
3. To define acceptable and unacceptable use of IT resources by all members of the University community.
4. To protect the University, its staff, students and stakeholders from legal, financial and reputational risk arising from misuse of IT resources.
5. To ensure compliance with applicable statutory, regulatory and contractual obligations.
6. To promote responsible digital citizenship and data privacy awareness across the University.

3. Scope and Applicability

This Policy applies to:

- All faculty, staff (teaching and non-teaching), officers and administrators of the University.
- All students enrolled in any programme of the University, including distance and online learners.
- Visiting faculty, guest lecturers, consultants, contractors, vendors and interns.
- Any individual or entity granted access to University IT resources, including affiliated colleges and research centres.

This Policy covers all IT resources owned, leased, licensed, or administered by the University, including but not limited to computers, servers, laptops, mobile devices, networks (wired and wireless), Internet and email services, software, cloud services, websites, learning management systems (LMS), ERP/student information systems, data storage, and any device connected to the University network ("IT Resources").

4. Definitions

Term	Definition
IT Resources	All hardware, software, networks, data, cloud services and communication systems owned or managed by the University.
User	Any individual authorized to access University IT Resources, including students, employees and third parties.
Authorized Access	Access granted through official University credentials for legitimate academic or administrative purposes.
Confidential Data	Information whose unauthorized disclosure could cause harm, including personal data, examination data, financial records and research data.
Incident	Any event that compromises the confidentiality, integrity or availability of IT Resources.

Term	Definition
BYOD	Bring Your Own Device — personally owned devices used to access University IT Resources.

5. IT Governance Structure

The University shall constitute an IT Governance Committee (ITGC), chaired by a senior official designated by the Vice-Chancellor, with representation from academic departments, administration, finance and the IT Department. Responsibilities of the ITGC include:

- Approving and periodically reviewing this Policy and related IT procedures.
- Overseeing IT infrastructure planning, budgeting and major procurement decisions.
- Reviewing security incidents and approving corrective action plans.
- Ensuring compliance with statutory and regulatory requirements.

The IT Department / IT Services shall be responsible for day-to-day administration, maintenance, security monitoring and technical support of IT Resources, and shall report to the ITGC.

6. Account and Access Management

6.1. User Accounts

Every user shall be issued a unique University account (username/ID) for accessing email, Wi-Fi, LMS, ERP and other systems. Accounts are non-transferable and must not be shared under any circumstances.

6.2. Password Requirements

- Passwords must be at least 8 characters long and include a combination of uppercase, lowercase, numeric and special characters.
- Passwords must not be shared, written down in plain view, or reused across multiple systems.

- Passwords must be changed immediately if compromise is suspected, and periodically as prescribed by IT Services.
- Multi-factor authentication (MFA) shall be enabled for email, ERP, financial systems and other critical applications wherever technically feasible.

6.3. Access Control

Access to systems and data shall be granted on the principle of least privilege — users shall be granted only the access necessary to perform their role. Access rights shall be reviewed periodically and revoked immediately upon change of role, resignation, expulsion, retirement or end of engagement.

7. Acceptable Use of IT Resources

University IT Resources are provided primarily for academic, research and administrative purposes. Users must act responsibly, ethically and lawfully at all times. Acceptable use includes:

- Using IT Resources for teaching, learning, research, official communication and University-related administrative work.
- Reasonable, incidental personal use of email and Internet, provided it does not interfere with official duties, consume excessive bandwidth, or violate this Policy.
- Reporting any observed vulnerabilities, misuse or suspicious activity to IT Services promptly.

8. Prohibited Activities

The following activities are strictly prohibited on any University IT Resource:

- Unauthorized access to, or attempts to access, another user's account, data or systems (“hacking”).
- Introducing, creating or distributing viruses, malware, ransomware or other malicious code.
- Sharing account credentials, or attempting to bypass authentication, firewall or security controls.

- Using University IT Resources to send spam, phishing messages, chain letters or unsolicited bulk communication.
- Downloading, storing, transmitting or displaying obscene, pornographic, defamatory, discriminatory or unlawful content.
- Harassment, cyberbullying, stalking, or any form of online abuse directed at students, staff or third parties.
- Unauthorized copying, distribution or use of copyrighted material, software piracy, or installation of unlicensed software.
- Using University networks or resources for commercial activity, political campaigning, or personal financial gain, without written authorization.
- Connecting unauthorized servers, wireless access points, or network devices that interfere with University network operations.
- Any activity that violates Indian law, including the Information Technology Act, 2000, or infringes the rights of any individual or organization.

Violation of these provisions may result in disciplinary action under Section 16 of this Policy, in addition to any civil or criminal liability under applicable law.

9. Email and Communication Policy

- Official University email accounts shall be used for all official academic and administrative correspondence.
- Users are responsible for all activity conducted through their assigned email account.
- Impersonation of another person or the University in electronic communication is strictly prohibited.
- Users must exercise caution with email attachments and links from unknown or suspicious sources to prevent phishing and malware attacks.
- Mass mailing / bulk communication on behalf of the University requires prior approval from the competent authority.

10. Internet and Network Usage

- Access to the University's wired and wireless networks is provided for academic and official purposes and is subject to monitoring and bandwidth management.
- Users shall not attempt to circumvent network security controls, content filters, or bandwidth restrictions.
- Peer-to-peer file sharing of copyrighted material and excessive recreational streaming that degrades network performance for others is prohibited.
- Guest and visitor network access shall be provided only through designated guest networks with appropriate authentication.

11. Data Security, Backup and Classification

11.1. Data Classification

University data shall be classified as Public, Internal, Confidential, or Restricted, and handled according to the sensitivity of each category.

11.2. Data Protection

- Confidential and Restricted data (examination records, personal data, financial and HR records, research data) must be stored only on authorized, secured systems.
- Removable media and portable devices used to store confidential data must be encrypted.
- Data must not be transferred to personal cloud storage or third-party services without authorization from IT Services.

11.3. Backup and Recovery

The IT Department shall maintain a documented backup schedule for critical systems (ERP, LMS, email, examination and financial systems) and shall periodically test data restoration procedures. A Business Continuity and Disaster Recovery Plan shall be maintained and reviewed annually.

12. Software and Hardware Management

- Only licensed and authorized software may be installed on University-owned computing devices.
- Installation of software on University systems requires prior approval from IT Services.
- The IT Department shall maintain an inventory (asset register) of all IT hardware and software licenses.
- Disposal of IT hardware shall follow secure data-wiping procedures and applicable e-waste management regulations.
- Personal software or hardware modifications to University-owned equipment are not permitted without authorization.

13. Bring Your Own Device (BYOD) and Remote Access

- Personally owned devices connecting to University networks or systems must comply with minimum security requirements prescribed by IT Services (updated operating system, antivirus, screen lock, etc.).
- Remote access to University systems (e.g., VPN, cloud applications) must use approved, secure methods and multi-factor authentication where available.
- The University reserves the right to restrict or revoke network access for any device found to pose a security risk.

14. Website, Social Media and Digital Content

- Content published on the official University website or social media handles must be accurate, approved by the competent authority, and consistent with the University's values and branding guidelines.
- Departments/individuals shall not create unofficial pages or accounts claiming to represent the University without prior authorization.
- Use of the University's name, logo or emblem on any digital platform requires prior written permission.

15. Privacy and Data Protection

- The University shall collect, process and store personal data of students, staff and other stakeholders only for legitimate academic, administrative or statutory purposes, consistent with applicable data protection law.
- Access to personal data shall be restricted to authorized personnel on a need-to-know basis.
- The University shall implement reasonable technical and organizational safeguards to protect personal data against unauthorized access, alteration, disclosure or destruction.
- Monitoring of IT Resources (network traffic, email systems, Internet usage) may be conducted by the University for security, compliance and operational purposes, in accordance with applicable law and with due regard to individual privacy.

16. Incident Reporting and Disciplinary Action

16.1. Incident Reporting

Any suspected security incident, data breach, loss/theft of a University device, or misuse of IT Resources must be reported immediately to IT Services through the designated helpdesk/incident reporting channel.

16.2. Investigation

The IT Department, in coordination with the ITGC and relevant disciplinary authority, shall investigate reported incidents. Users are required to cooperate fully with any authorized investigation.

16.3. Disciplinary Action

Violation of this Policy may result in disciplinary action as per applicable University Statutes/Ordinances/service rules and student conduct regulations, ranging from warning, suspension of IT access, fines, suspension/expulsion (for students) or termination (for employees), in addition to referral to law enforcement authorities where the violation constitutes a criminal offence.

17. Roles and Responsibilities

Role	Key Responsibilities
IT Governance Committee	Policy approval, oversight, risk review, budget approval for major IT initiatives.
IT Department / IT Services	Infrastructure management, security monitoring, technical support, incident response, backups.
Heads of Department / Deans	Ensuring compliance within their department; recommending access requirements for staff/students.
Employees	Complying with the Policy; safeguarding credentials and assigned devices; reporting incidents.
Students	Using IT Resources responsibly for academic purposes; complying with acceptable use rules.
System/Data Owners	Classifying data under their charge and defining access requirements.

18. Exceptions

Any request for an exception to this Policy must be submitted in writing to the IT Governance Committee, stating the business/academic justification, scope and duration. Exceptions shall be granted only where compensating controls are in place and shall be documented and reviewed periodically.

19. Policy Review

This Policy shall be reviewed by the IT Governance Committee at least once every two years, or earlier if warranted by changes in law, technology, or institutional requirements. Amendments shall be approved by the competent authority of the University and communicated to all stakeholders.

20. Acknowledgement

All users of University IT Resources are required to read, understand and acknowledge acceptance of this Policy at the time of onboarding (admission/employment) and upon any material revision, as a condition of being granted access to University IT Resources.

Issued under the authority of the Vice-Chancellor, Sharnbasva University.