Digital Personal Data Protection (DPDP)

Policy

Lakireddy Bali Reddy College of Engineering
(Autonomous)
Mylavaram – 521 230

1. Preamble

In compliance with the Digital Personal Data Protection Act, 2023, the Institution is committed to protecting the privacy and personal data of its stakeholders. This policy establishes a structured framework for the lawful, transparent, and secure processing of personal data, ensuring accountability and trust in institutional data practices.

2. Purpose of the Policy

The objectives of this policy are to:

- Ensure compliance with the DPDP Act, 2023
- Protect the personal data of students, staff, faculty, alumni, applicants, and other stakeholders
- Establish data governance, security safeguards, and grievance redressal mechanisms
- Prevent unauthorized access, misuse, or data breaches

3. Scope and Applicability

This policy applies to:

- All personal data processed digitally or digitized from physical records
- All departments, units, and affiliated centers of the Institution
- All stakeholders, including students, employees, alumni, vendors, and visitors

4. Definitions

For the purpose of this policy:

- **Personal Data**: Any data about an identifiable individual
- **Data Principal**: Individual to whom the personal data relates
- **Data Fiduciary**: The Institution, which determines the purpose and means of processing personal data
- **Data Processor**: Any entity processing data on behalf of the Institution
- **Consent**: Freely given, specific, informed, and unambiguous indication of agreement

5. Data Protection Governance

5.1 Data Protection Committee (DPC)

The Institution shall constitute a **Data Protection Committee** comprising:

- Head of Institution – Chairperson
- **Data Protection Officer (DPO)** – Convener
- IT Head / System Administrator
- Legal / Compliance Officer
- Administrative Representative

5.2 Roles and Responsibilities

- **Data Protection Officer (DPO)**:
    - Ensure compliance with DPDP Act, 2023
    - Act as the contact point for data principals
    - Monitor data processing activities
    - Report data breaches and corrective actions
- **Departments**:
    - Ensure data accuracy and minimization
    - Follow approved data retention schedules

6. Principles of Data Processing

The Institution shall process personal data based on the following principles:

1. Lawfulness and Fairness
2. Purpose Limitation
3. Data Minimization
4. Accuracy and Quality
5. Storage Limitation
6. Security Safeguards
7. Accountability

7. Consent Management

- Consent shall be obtained before collecting personal data, except where legally permitted
- Clear privacy notices shall be provided at the time of data collection
- Data principals may withdraw consent and request correction or erasure of data

8. Rights of Data Principals

The Institution shall ensure:

- Right to access personal data
- Right to correction and erasure
- Right to grievance redressal
- Right to nominate a representative

9. Data Security Measures

- Role-based access control
- Secure authentication mechanisms
- Encryption of sensitive data
- Regular data backups
- Periodic security audits and vulnerability assessments

10. Data Breach Management

- Immediate reporting of data breaches to the DPO
- Assessment of impact and mitigation
- Intimation to affected data principals and authorities, as applicable
- Maintenance of a data breach incident register

11. Data Sharing and Third-Party Compliance

- Data sharing only through formal agreements
- Due diligence of third-party vendors
- Inclusion of DPDP compliance clauses in MoUs and contracts

12. Data Retention and Disposal

- Data retained only for the period necessary to fulfill institutional and legal requirements
- Secure deletion or anonymization of data after the retention period

13. Awareness and Training

- Periodic data protection and cyber security awareness programs
- Training for staff and faculty handling personal data

14. Grievance Redressal Mechanism

- Data principals may submit grievances to the DPO
- Grievances shall be addressed within the stipulated time
- Escalation to the **Data Protection Board of India**, if required

15. Monitoring, Audit, and Review

- Periodic internal audits for DPDP compliance
- Annual review of this policy
- Amendments as per Government or regulatory updates

The Institute shall continuously review and update the approved policy and is committed to its implementation.

Policy History:

Version	Approved by	Implementation and Monitoring by
V1.0(Original)	20th Meeting of GB held on 31-01-2026	Dean (Academics)