Standard Operating Procedure (SOP): Confidentiality and Student Records Management

This SOP details **confidentiality and student records management**, encompassing the proper handling, storage, access, and sharing of student information to ensure privacy and compliance with legal and institutional requirements. It includes guidelines for protecting sensitive data, managing electronic and physical records, authorized personnel access, record retention and disposal, as well as procedures for responding to data breaches to maintain the integrity and confidentiality of all student records.

1. Purpose

To establish clear procedures for managing the confidentiality, security, and integrity of student records in compliance with applicable laws (e.g., FERPA), regulations, and institutional policies.

2. Scope

This SOP applies to all employees, contractors, and authorized personnel who handle, process, or access student records in any format (electronic or paper) within the institution.

3. Definitions

Term	Definition
Student Records	Any information directly related to a student and maintained by the institution, including academic, personal, and disciplinary records.
Confidential Information	Data that is protected by law, policy, or procedure from unauthorized access, disclosure, alteration, or destruction.
Authorized Personnel	Individuals who have received formal approval to access student records as necessary for their job functions.
Data Breach	Unauthorized access, use, disclosure, or loss of sensitive student information.

4. Roles and Responsibilities

- **Registrar/Records Office:** Oversees student records management and compliance.
- **IT Department:** Ensures the security of electronic records systems.
- **All Employees:** Responsible for safeguarding student information per this SOP.
- **Data Protection Officer:** Handles data breaches and compliance concerns.

5. Procedures

5.1 Handling of Student Records

- Only authorized personnel may access student records.
- Records must be accessed solely for legitimate educational or administrative purposes.
- Records should not be modified, destroyed, or shared without proper authorization.

5.2 Storage of Records

- Physical records must be stored in locked cabinets or secure areas.
- Electronic records must be protected by passwords, encryption, and access controls.
- Access logs should be maintained for both physical and electronic records.

5.3 Sharing and Disclosure

- Student information may only be shared with authorized individuals with a defined need-to-know.
- External requests (e.g., from parents or third parties) require written consent from the student or as permitted by law.
- All disclosures must be documented.

5.4 Record Retention and Disposal

- Records must be retained according to institutional and legal retention schedules.
- Expired records must be disposed of securely (e.g., shredding for paper, secure deletion for electronic files).
- Disposal actions should be documented.

5.5 Data Breach Response

- Any suspected or actual data breach must be reported immediately to the Data Protection Officer.
- Contain the breach, assess risks, notify affected parties, and remediate per institutional policy.
- A breach report must be completed, and preventive actions implemented.

6. Training and Compliance

- All personnel handling student records must receive regular training on confidentiality and data security practices.
- Non-compliance may result in disciplinary action, up to and including termination.

7. Revision and Review

- This SOP will be reviewed annually or as required by changes in laws and policies.
- Revisions must be approved by the Registrar and the Data Protection Officer.

8. References

- Family Educational Rights and Privacy Act (FERPA)
- Institutional Records Management Policy
- Data Protection Laws and Regulations

Approved by: [Name/Title]
Date: [Date of Approval]