Standard Operating Procedure (SOP)
Student Records Confidentiality and Privacy Compliance

This SOP defines the policies and procedures for maintaining **student records confidentiality and privacy compliance**, including guidelines for the secure collection, storage, access, and sharing of student information. It ensures adherence to legal and institutional requirements such as FERPA, promotes responsible handling of personal data, and outlines protocols for breach response and training to protect student privacy at all times.

1. Purpose

To establish standardized procedures to protect the confidentiality and privacy of student records in compliance with federal (FERPA), state, and institutional regulations.

2. Scope

This SOP applies to all employees, faculty, contractors, and volunteers who collect, access, use, or manage student records and information at the institution.

3. Definitions

- **Student Records:** Any information directly related to a student and maintained by the institution or party acting for the institution.
- **Personally Identifiable Information (PII):** Information that can identify a student, such as name, address, student number, or other unique identifiers.
- **FERPA:** The Family Educational Rights and Privacy Act, a federal law protecting the privacy of student education records.

4. Policy Statements

- Student records must be collected, accessed, used, and disclosed only as necessary and as permitted by law.
- All staff must adhere to institutional, state, and federal privacy regulations.
- Unauthorized use or disclosure of student records is strictly prohibited and subject to disciplinary action.

5. Procedures

5.1 Collection of Student Information

- Collect only the minimum information necessary for legitimate institutional purposes.
- Obtain student consent if required, and inform students about the collection and intended use of their information.

5.2 Storage and Security

- Store physical records in secure, access-controlled locations.
- Store electronic records in encrypted and password-protected systems compliant with IT security policies.

5.3 Access Control

- Grant access to student records only to authorized personnel with a legitimate educational interest.
- Regularly review user access and promptly revoke access upon role changes or separation from the institution.

5.4 Data Sharing and Disclosure

- Release student information externally only with proper consent or as allowed by law (e.g., in response to a subpoena, emergency, or directory requests).
- Document all disclosures in accordance with FERPA requirements.

5.5 Data Retention and Disposal

- Retain student records only for the period required by institutional policy or law.
- Dispose of student records securely (e.g., shredding physical documents, permanently deleting electronic files).

6. Incident/Breach Response

- Immediately report any suspected or actual breach of student records to the institution's designated Data Protection Officer and IT department.
- Follow the institutional incident response plan, including notification, investigation, mitigation, and documentation steps.

7. Training and Awareness

- All personnel must complete annual training on student privacy and data protection requirements.
- Regular updates and awareness campaigns shall be conducted to reinforce compliance and best practices.

8. Responsibility

- All staff, faculty, and third-party service providers are responsible for adhering to this SOP.
- The Data Protection Officer or Registrar is responsible for oversight and ensuring update and enforcement of this SOP.

9. Review and Revision

- This SOP shall be reviewed annually or upon regulatory changes to ensure ongoing compliance.

10. References

- FERPA Regulations
- Institutional Data Privacy Policy
- Applicable State Regulations

Document Control:
SOP Number: SR-Conf-Privacy-01
Version: 1.0
Effective Date: [Insert Date]
Next Review Date: [Insert Date]