STUDENT CONFIDENTIALITY AND PRIVACY POLICY

Prepared by:	Reviewed by:	Approved by:
Melissa Huayanca Acleto  Karen Rocío Galeano Villada 	Melissa Huayanca Acleto  Diana Cecilia Zapata Fernandez 	Carolina Barrios Verand 
Date: 24/09/2025	Date: 24/09/2025	Date: 24/09/2025

Printing or copying this document results in it becoming an "UNCONTROLLED DOCUMENT."

1. PURPOSE

The purpose of this policy is to protect the privacy of student information and ensure it is collected, stored, and used responsibly in compliance with applicable laws. It applies to all students, faculty, staff, and third parties who access or process student data, including academic, personal, financial, health, and digital records. The policy safeguards against unauthorized access or disclosure and promotes trust, accountability, and respect for student rights.

2. SCOPE

This policy applies to all students of the institution, as well as faculty, staff, and third parties who handle student information. It covers all forms of student data, including academic, personal, financial, health, and digital records, regardless of format or storage system.

3. REGULATORY FRAMEWORK

This policy considers the following external and internal regulations to ensure quality:

- Non-Discrimination Law (Title VI, Title IX, ADA): “U.S. Department of Justice. (1964). Civil Rights Act of 1964.”
- Inclusion and Diversity Policies in Schools: “U.S. Department of Education. (2020). The Civil Rights Data Collection (CRDC).”
- Diversified Student Experience: “U.S. Department of Education. (2021). Guidelines for promoting student diversity in higher education.”
- Multicultural Education and Cultural Sensitivity: “U.S. Department of Education. (2019). Cultural competence standards in education.”
- Diversity in Hiring and Academic Programs: “U.S. Equal Employment Opportunity Commission. (2021). Affirmative Action and Equal Opportunity Employment.”
- Support Programs for Students from Vulnerable Groups: “U.S. Department of Education. (2020). Individuals with Disabilities Education Act.”
- Privacy and Data Protection Law (FERPA): “U.S. Department of Education. (2021). Family Educational Rights and Privacy Act (FERPA).”
- Professional Experience and Volunteering Programs: “U.S. Department of Labor. (2021). Youth Employment and Labor Standards.”
- Digital Accessibility and Inclusion: “U.S. Access Board. (2021). Section 508 Standards and Guidelines.”
- USA: Florida Digital Bill of Rights (FDBR).
- Peru: Compliance with Law No. 29733 on Personal Data Protection (ARCO rights: Access, Rectification, Cancellation, Opposition).
- Colombia: Compliance with Law 1581 of 2012 and Decree 1377 of 2013, requiring explicit authorization for data processing and transfer.
- Ecuador: Compliance with the Organic Law on Personal Data Protection (LOPDP), including rights of access, correction, deletion, opposition, and portability.

4. DEFINITIONS AND TERMS

- Academic Advisor: Professional responsible for providing academic guidance, monitoring, orientation, and referrals as needed.
- Academic Fee: Refers to the payment that must be made for the requested document.

- Academic Regulations: Formal document that sets out the obligations, benefits, and sanctions of the members of the university community in order to guide their conduct, establish academic processes, and foster a harmonious environment.
- Banner: Enterprise Resource Planning (ERP) software designed for higher education, used by the university as its academic management system.
- CFU Service Model: A case-typification system to structure student requests and interactions with university services.
- Course/Period Withdrawal: Process to drop courses/periods, possibly resulting in a “W” (withdrawal) or “F” (fail).
- Educational Model: A compilation or synthesis of different theories and pedagogical approaches that guide teachers in the development of study programs and in the systematization of the teaching and learning process.
- Enrollment Deferral (Reservation): Procedure to temporarily postpone studies while retaining a place.
- FERPA: U.S. federal law protecting the privacy of student records.
- Help Center: Institutional digital platform where student requests for administrative, documentary, or academic procedures are registered.
- Shared Folder: A set of files held exclusively by the Academic Records department, which are shared only within that area.
- SLA (Service Level Agreement): Defines response and service times for student requests.
- Student Experience: The set of services, activities, interactions, and support a student receives throughout their academic life and alumni stage.
- Student in Abandonment: Student who accumulates 10% or more consecutive absences without formal withdrawal.
- Student Services: Areas of support such as well-being, academic advising, financial aid, employability, technology, among others.
- Student Typification: Institutional classification of students based on academic status (e.g., new, regular, reinstated, withdrawn, suspended, expelled).

5. GENERAL POLICY AND GUIDELINES

5.1. Policy Statement

Continental Florida University is committed to protecting the confidentiality, integrity, and privacy of all student information. Personal, academic, and administrative data entrusted to the Institution will be collected, stored, and used only for legitimate academic, administrative, and legal purposes. The Institution guarantees that such information will not be shared with unauthorized parties and will always be handled with respect, fairness, and responsibility.

5.2. Collection and Use of Information

Student information is collected only for purposes directly related to academic administration, student services, and compliance with legal requirements. The Institution ensures that such data will not be used for commercial or non-academic purposes unless explicit written consent has been obtained from the student. Information provided by students will be treated as confidential and will be processed in a manner that upholds the highest standards of data protection.

CFU’s confidentiality and privacy framework is guided by the following principles:

- **Transparency:** Individuals are informed of how their data will be used.
- **Informed Consent:** No personal data is collected without prior, free, and explicit authorization.
- **Legitimate Purpose:** Data is processed solely for academic, administrative, legal, or institutional purposes.

- **Proportionality:** Only the minimum information necessary is collected.
- **Security:** Technical, physical, and organizational safeguards are in place to protect data integrity, confidentiality, and availability.

5.3. Categories of Data Collected

- **Identification Data:** Full name, identification number, nationality, date of birth.
- **Contact Data:** Email, phone number, address, country of residence.
- **Academic and Employment Data:** Educational background, transcripts, program applications, employment history.

- **Sensitive Data (when required):** Medical information, marital status, dependents (for scholarship or legal purposes).
- **Technical Data:** IP address, browser, cookies, logins, web interactions.
- **Marketing and Communication Data:** Preferences, surveys, campaign responses.
- **User-Generated Content:** Academic submissions, forum posts, participation in online platforms.

5.4. Purposes of Data Processing

Data is processed to:

- Manage admissions, scholarships, academic records, and student services.
- Provide academic and administrative advising.
- Operate virtual classrooms, events, and related academic activities.
- Ensure compliance with legal and regulatory obligations.
- Conduct institutional research and quality improvement.
- Carry out marketing, communication, and outreach activities (always with prior consent).

5.5. Consent Management

- All web and enrollment forms include a non-preselected opt-in checkbox for acceptance of data processing.
- In chats, WhatsApp, and virtual events, CFU provides prior notice and direct access to the Privacy Policy.
- Consent is tracked and stored in institutional systems for accountability.
- Consent mechanisms are applied in student forms and in the student census.

5.6. Security Measures

The Institution is committed to implementing robust security measures to protect student information against unauthorized access, alteration, or misuse. Digital records will be safeguarded through appropriate technological controls, such as encryption, secure passwords, and restricted system access. Physical records will be stored in secure locations with access granted only to authorized personnel. These measures are designed to ensure the integrity and confidentiality of all student data.

CFU implements technical, administrative, and physical safeguards to protect personal data, including:

- Encrypted storage and transmission of sensitive data.
- Secure servers located in the United States.
- Role-based access control and confidentiality agreements for authorized staff.
- Regular system monitoring, backups, and vulnerability assessments.
- Authentication and audit logs within academic and CRM platforms.

5.7. Confidentiality and Access Control

Access to student records is strictly limited to authorized faculty and staff who require the information to perform their academic or administrative responsibilities. Students are entitled to access their own records upon request and may petition for the correction of any inaccurate or incomplete information. The disclosure of student data to third parties is prohibited unless written authorization has been provided by the student, or unless disclosure is required by law or institutional regulation.

5.8. Responsibilities

The protection of student confidentiality and privacy is a shared responsibility. The Institution is responsible for developing secure systems, providing training to staff and faculty, and monitoring compliance with this policy. Faculty and staff are required to respect and maintain the confidentiality of student records and are prohibited from misusing or disclosing information. Students are responsible for providing accurate personal and academic information and for respecting the privacy of their peers.

5.9. Rights of Students

Students have the right to access their personal and academic records and to request the correction of any inaccuracies. They also have the right to be informed about the collection, use, and purpose of their data. Furthermore, students may file a complaint if they believe that their privacy rights have been violated, and the Institution commits to investigating and addressing such complaints promptly and fairly.

5.10. Violations and Sanctions

Any violation of this policy, whether by students, faculty, or staff, will be treated with the utmost seriousness. Breaches may result in disciplinary action, including but not limited to suspension, termination of employment, or referral to legal authorities, depending on the nature and severity of the infraction. These sanctions are intended to reinforce the Institution's commitment to safeguarding student confidentiality and privacy at all times.

6. APPENDIX

Code	Appendix	Validity
POL02.SU03-DOC1	Typification Matrix	1 year
POL02.SU03-DOC2	Informed Consent Form	Indefinite
POL02.SU03-DOC3	User Access Matrix	1 year
POL02.SU03-DOC4	Student Information Backup	1 year

7. VERSION CONTROL

N°	Requested by	Changes Control
1.0	Executive Director	Initial document

Printing or copying this document results in it becoming an "UNCONTROLLED DOCUMENT."