CELESTE BEAUTY ACADEMY, INC.
IT-104 STUDENT DATA PRIVACY AND FERPA COMPLIANCE

Policy ID	IT-104	**Version**	1.0
Board Approval Date (Version 1.0)	November 15, 2026	**Date of Last Review**	
Statutory / Regulatory References	FERPA, 20 U.S.C. § 1232g; 34 C.F.R. Part 99; N.C. Gen. Stat. Ch. 115C, including applicable student data privacy provisions.		

Protect student education records and personally identifiable information (PII) and establish procedures for access, disclosure, parent/eligible-student rights, and approved technology. Applies once CBA maintains education records and to pre-enrollment data where other privacy obligations apply.

I. DEFINITIONS

Education records are records directly related to a student and maintained by CBA or a party acting for it, subject to FERPA exclusions. An eligible student is generally a student who has turned 18 or attends a postsecondary institution. Directory information may be disclosed only after proper notice and an opportunity to opt out, if CBA adopts such a designation.

II. ACCESS AND LEGITIMATE EDUCATIONAL INTEREST

Limit access to school officials with legitimate educational interests under FERPA and documented Academy criteria. Authenticate identity before providing records. Maintain role-based access and review permissions when assignments change.

III. PARENT AND ELIGIBLE STUDENT RIGHTS

Provide required annual FERPA notification. Allow eligible parents and students to inspect and review education records within FERPA's 45-day period, request amendment of records believed inaccurate or misleading, receive a hearing when required, and file a complaint with the U.S. Department of Education. Follow legal rules governing transfer of rights at age 18.

IV. CONSENT AND PERMITTED DISCLOSURES

Obtain signed and dated written consent before disclosing PII from education records unless a FERPA exception applies. Document the basis for exceptions, such as disclosure to qualifying school officials, transfers to another school, health/safety emergencies, or other permitted circumstances. Do not assume all contractors qualify as school officials.

V. RECORD OF DISCLOSURES

Maintain FERPA disclosure records when required, including the requesting party and legitimate interest, and observe applicable exceptions to logging. Keep records with the relevant education record as required.

VI. DIRECTORY INFORMATION AND PUBLICITY

CBA will not disclose student directory information under the directory-information exception unless it first adopts categories, issues annual notice, and provides a reasonable opt-out period. Obtain appropriate photo/media permissions for promotional use; a publicity release does not override FERPA requirements.

VII. ONLINE SERVICES AND VENDORS

Review educational technology vendors for data minimization, direct control, authorized educational use, security, subcontracting, retention, and return/deletion. Comply with applicable North Carolina student-data laws and contract requirements. Prohibit vendor use of student records for behavioral advertising or unauthorized commercial purposes.

VIII. RECRUITMENT VS. OFFICIAL APPLICATIONS

Keep informal website and Meta lead forms separate from official enrollment and education records. Do not upload education records or sensitive student information to advertising platforms. Interest submissions must not confer preference in CBA's weighted admissions lottery.

IX. SECURITY, INCIDENTS, AND RETENTION

Apply IT-102 security controls and IT-105 incident procedures. Retain and dispose of student records under applicable North Carolina records schedules, legal holds, and federal requirements; deletion requests do not override mandatory retention.

X. TRAINING, COMPLAINTS, AND REVIEW

Train personnel with student-record access before access and at least annually. Refer FERPA questions to the designated records/privacy officer at President@celestebeautyacademy.com until a specific officer is appointed. Review annually and after material changes in law.

Implementation and Approval

This draft establishes proposed requirements. CBA shall identify responsible personnel, verify current technology and vendor practices, and obtain legal review before adoption. Management shall develop supporting procedures, forms, and training as needed. Nothing in this policy supersedes applicable law or an approved records retention schedule.