CELESTE BEAUTY ACADEMY, INC.
IT-103 ACCEPTABLE USE OF TECHNOLOGY

Policy ID	IT-103	**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; Children's Internet Protection Act, 47 U.S.C. § 254(h), where applicable; N.C. Gen. Stat. Ch. 115C.		

Define responsible use of Academy-owned or Academy-managed accounts, devices, networks, applications, and communications by staff, board members, contractors, volunteers, and students where applicable. Student-specific rules may be supplemented by the student handbook.

I. AUTHORIZED USE

Use Academy technology primarily for legitimate educational and operational activities. Limited incidental personal use may be permitted for staff if lawful, minimal, and not disruptive, unless management prohibits it. Users must comply with applicable law, Academy policies, and licensing terms.

II. ACCOUNT RESPONSIBILITIES

Protect passwords and authentication factors; never share credentials or use another person's account. Lock devices when unattended. Immediately report suspected account compromise, lost devices, or accidental disclosure to the designated IT/security contact.

III. PROHIBITED ACTIVITIES

Do not harass, threaten, discriminate, access unlawful material, circumvent security controls, install unapproved software, mine cryptocurrency, conduct unauthorized commercial or political campaign activities using school resources, or access information without a legitimate role-based need.

IV. EMAIL, SOCIAL MEDIA, AND PUBLIC COMMUNICATIONS

Use approved CBA accounts for school business. Only designated personnel may publish on official CBA social media or run advertising campaigns. Do not post student images, identifying details, or educational information without the required authorization and applicable permissions. Follow records-retention and public-records obligations for official communications.

V. STUDENT AND FAMILY INFORMATION

Do not transmit student records through personal accounts or unapproved applications. Use approved platforms and check recipient addresses before sending. Never use student information for personal outreach, advertising audience uploads, or unrelated marketing.

VI. AI AND THIRD-PARTY APPLICATIONS

Obtain authorization before connecting new apps or AI tools to Academy accounts. Do not enter Restricted or confidential information into public AI tools without approved safeguards and a documented permissible use.

VII. NETWORK AND DEVICE CARE

Install updates when directed; do not disable antivirus, device management, or filtering controls. Connect only approved devices where required. Return Academy equipment and records when service or employment ends.

VIII. MONITORING AND PRIVACY

To the extent permitted by law, CBA may review use of its systems for security, compliance, operational continuity, and public-records purposes. Users should not assume personal privacy in Academy systems; monitoring must itself comply with law and Academy policy.

IX. STUDENT SAFEGUARDS AND ACCESSIBILITY

CBA will apply age-appropriate internet safety and filtering measures where required, including applicable Children's Internet Protection Act requirements if triggered by funding. Users must follow accessibility, anti-bullying, and student conduct rules.

X. VIOLATIONS AND REVIEW

Suspected misuse must be reported. CBA may restrict access pending investigation and apply proportionate consequences consistent with applicable procedures. Review annually.

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.