

STILLMAN COLLEGE POLICY & PROCEDURE

Policy Name:
PRIVACY PROTECTION FOR
ONLINE STUDENTS

Approved by: Yolanda W. Page
President Yolanda W. Page (Sep 8, 2026 17:17:46 CDT)

College Division:
Institutional Effectiveness and
Research

Date Established:
5/22/18

Date Revised:
08/27/26

Date Removed:
N/A

Policy Statement

Stillman College defines an online student as a student who receives all or part of their instruction in a location separate from the instructor. This policy applies to all distance education courses and programs offered by the institution. Stillman College does not offer correspondence education.

Stillman College ensures that the student who registers in a distance education course or program is the same student who participates in, completes the course or program, and receives academic credit. Student identity is initially verified during the admissions process through the submission of required official transcripts and state-issued photo identification.

Once admitted, each student is assigned a unique seven-digit student identification number (SID). Initial credentials are issued individually by Information Technology and must be reset at first login. Upon first logging into the Stillman email platform, students are prompted to reset their password and enroll in 2-step verification within seven days to further protect their login credentials. If they fail to enroll in 2-step verification within the time allotted, they will be locked out of their Stillman email account and must contact Information Technology for verification and assistance.

Student identification numbers are managed in the College's Enterprise Resource Planning system (ERP). Student email usernames and passwords are managed through the College's Identity and Access Management system (IAM). Both systems are accessible only to authorized personnel through secure, password-protected login portals, thereby protecting the privacy of all students, including online students, in full compliance with the Family Educational Rights and Privacy Act (FERPA).

Other institutional platforms, including the College's Learning Management System (LMS), are accessible through single sign-on (SSO) using the student's Stillman email account. Access to the LMS is granted only after an account has been created in the LMS Admin Portal.

Students are responsible for safeguarding their SID, username, and password. They are strongly discouraged from sharing this information with others, as doing so violates the College's Academic Dishonesty Policy.

Stillman College is committed to protecting the privacy, confidentiality, and security of student records and personally identifiable information in all online learning environments, including learning management systems, video conferencing platforms, online assessment tools, proctoring services, and other approved instructional technologies.

Purpose

The purpose of this policy is to establish procedures that protect the privacy of students enrolled in distance education courses and programs and to ensure that Stillman College verifies the identity of online students in accordance with federal regulations, FERPA, and applicable accreditation requirements.

This policy is intended to:

- Protect the privacy of online students;
- Safeguard student educational records and personally identifiable information;
- Verify that the student who registers for an online course is the same student who participates in and completes the course;
- Ensure secure access to College technology resources;
- Define student, faculty, staff, and institutional responsibilities; and
- Maintain compliance with FERPA and applicable institutional, state, federal, and accreditation requirements.

Scope

This policy applies to:

- All students enrolled in online, hybrid, or distance education courses;
- Faculty teaching online, hybrid, or distance education courses;
- Staff with access to online student records or instructional platforms;
- Administrators responsible for distance education, information technology, student records, or compliance;
- College-approved learning management systems and instructional technologies;
- Third-party vendors or service providers that support online learning; and
- Any system that stores, processes, transmits, or provides access to online student information.

Definitions

For the purpose of this policy:

Online Student means a student who receives all or part of their instruction in a location separate from the instructor.

Distance Education means instruction delivered through technology to students who are separated from the instructor and that supports regular and substantive interaction between the students and instructor.

Personally Identifiable Information, or PII, means information that can be used to distinguish or trace a student's identity, either directly or indirectly.

Education Record means records that are directly related to a student and maintained by the College or by a party acting on behalf of the College.

Identity and Access Management System, IAM, means the College-approved centralized dashboard used by IT administrators to manage email user accounts, routing, aliases, and security rules for the entire College.

Learning Management System, or LMS, means the College-approved online platform used to deliver course content, assignments, grades, assessments, communication, and other instructional activities.

Single Sign-On, or SSO, means an authentication process that allows users to access multiple approved College systems using one set of secure credentials.

Third-Party Vendor means an external service provider approved by the College to support online learning, student services, technology, assessment, communication, or related operations.

Student Identity Verification means the process used by the College to confirm that the student who registers for a distance education course or program is the same student who participates in, completes the course or program, and receives academic credit.

Procedures for Implementation

Final admission to Stillman College requires students to provide a valid, state-issued photo identification card to verify their identity. Stillman College charges no fee at any point for verification of student identity. Students are notified in writing at the time of registration or enrollment that Stillman College charges no additional fees or projected charges for the verification of student identity.

Upon admission, each student is assigned a unique seven-digit Student Identification Number (SID), which is generated through the College's Enterprise Resource Planning (ERP) system. The Information Technology Department then establishes the student's official username and password for secure access to authorized College technology resources, including email and other institutional systems.

Personally identifiable information (PII) is maintained on secure College servers and protected through password-controlled access and two-step verification in accordance with FERPA guidelines. Access to student information is limited to authorized individuals based on their institutional roles and responsibilities.

To further protect student records, students are required to present their College-issued Student Identification Card when requesting access to academic, financial, or other official student records. These procedures help ensure that student information is accessed only by authorized individuals and support the College's commitment to privacy, security, and accurate identity verification.

FERPA Compliance

Stillman College complies with the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records.

In accordance with FERPA, students have the right to:

- Inspect and review their education records;

- Request amendment of inaccurate or misleading records;
- Provide written consent before personally identifiable information from education records is disclosed, except where FERPA permits disclosure without consent;
- Be informed annually of their FERPA rights; and
- File a complaint with the appropriate federal office regarding alleged FERPA violations.

Student education records, including records created or maintained through online learning platforms, are protected under FERPA. Access to such records is limited to College officials with a legitimate educational interest or as otherwise permitted by law.

Student Identity Verification

Stillman College verifies student identity through multiple secure processes, including but not limited to:

- Review of official admissions documents;
- Submission of valid, state-issued photo identification;
- Assignment of a unique Student Identification Number;
- Secure username and password credentials;
- Required password reset upon first login;
- Enrollment in 2-step verification;
- Single sign-on authentication for approved institutional systems; and
- Use of secure College technology platforms.

Students are responsible for maintaining the confidentiality of their login credentials and for immediately reporting any suspected unauthorized access to their accounts.

Stillman College does not charge students any additional fees for student identity verification. If any future identity verification method results in a student fee, the College will notify students in writing at the time of registration or enrollment.

Protection of Login Credentials

Students must protect their SID, username, password, and authentication information.

Students are prohibited from:

- Sharing login credentials with another person;
- Allowing another person to access College systems using their account;
- Using another student's account or credentials;
- Attempting to bypass authentication controls; or
- Misrepresenting their identity in an online course or assessment.

The College will never request a student's password through email. Students who believe their account has been compromised must immediately contact the Information Technology Department or Help Desk.

Account Recovery and Help Desk Identity Verification

Stillman College maintains a defined protocol for verifying the identity of any individual who requests assistance with account access. This protocol applies to all requests for password resets, two-step verification

resets, account unlocks, and restoration of access to college systems, whether the request is made in person, by telephone, or electronically.

Before any credential is reset or any account is unlocked, Information Technology staff verify the requester's identity. Verification requires the requester to provide multiple matching identifiers drawn from the student record maintained in the College's Enterprise Resource Planning system. Acceptable identifiers include the seven-digit Student Identification Number, full legal name as it appears in the student record, date of birth, the last four digits of the Social Security number, and the address of record. Requests made in person require the presentation of a valid College-issued or state-issued photo identification card.

Information Technology does not reset credentials based on an electronic request alone. A request received from an address or telephone number other than the contact information of record is not acted upon without independent verification of the requester's identity.

Reset credentials are never disclosed through unsecured channels. When a reset is completed, a temporary credential is delivered through the personal email address on file in the ERP, and the student is required to establish a new password upon first login and to re-enroll in two-step verification.

Every account access and credential reset request is logged in the College's Spiceworks ticketing system with the date of the request, the identity of the staff member who performed the verification, the identifiers used to verify the requester, and the action taken. These records are retained in accordance with the College's records retention schedule and are available for institutional audit and review.

A request that cannot be verified is denied, and the requester is directed to appear in person with photo identification at the office of Information Technology or to complete an alternative verification process approved by the Director of Information Technology. Any suspected attempt to obtain access to another individual's account is reported and handled as a privacy incident under the Privacy Incident and Breach Reporting section of this policy.

Collection and Use of Student Information

Stillman College may collect and use student information necessary to support enrollment, instruction, academic assessment, student services, institutional reporting, compliance, and security.

Information collected may include, but is not limited to:

- Student name;
- Student identification number;
- College email address;
- Course enrollment information;
- Course participation and attendance data;
- Assignment submissions;
- Grades and academic progress;
- Discussion board posts and messages;
- Assessment and quiz activity;
- LMS login and activity data;
- IP addresses, device information, and browser information when collected by institutional systems;
- Video, audio, chat, or screen-sharing data when using approved conferencing or proctoring tools; and

- Records necessary for academic support, advising, financial aid, or compliance purposes.

Student information is used only for legitimate educational, administrative, security, reporting, or compliance purposes.

Learning Management System Privacy and Security

The College's LMS is used to support instruction, communication, grading, course content delivery, and student engagement.

Access to the LMS is controlled through approved authentication processes, including SSO where applicable.

Access to LMS data is limited to authorized users, including students, assigned faculty, academic administrators, instructional support personnel, and authorized Information Technology staff.

LMS records, including grades, course activity, submitted assignments, and communication records, are considered education records and are protected in accordance with FERPA and institutional policies.

Online Proctoring and Assessment Security

Stillman College requires proctoring for major assessments administered in distance education courses.

Major assessments include midterm examinations, final examinations, and other summative assessments designated by the instructor of record or by the academic program.

Proctoring is administered through Proctorio, the College's approved examination proctoring service. The service is integrated with the College's Learning Management System and is accessed through single sign-on using the student's institutional credentials.

Prior to the start of a proctored assessment, the service verifies the identity of the test taker through authentication via single sign-on, capture of a live photograph of the test taker, comparison of that photograph against a government-issued photo identification presented at the time of the examination, and a recorded environment check. This verification confirms that the student who registers for a distance education course is the same student who completes its major assessments. Identity verification for major assessments therefore does not rest solely on the login credentials issued at the time of admission.

During a proctored session, the service may employ webcam monitoring, audio monitoring, screen monitoring, browser lockdown, or other College-approved assessment security methods. Sessions are recorded. Sessions flagged for irregularity are reviewed by the instructor and/or personnel in Information Technology and, where warranted, referred for action under the Academic Dishonesty Policy.

Students are notified of proctoring requirements, technology requirements, identity verification procedures, and the categories of data collected. Notification is provided in the course syllabus and in the Student Handbook.

Data collected through proctoring tools is used only for identity verification, academic integrity, assessment security, and compliance purposes. Such data is retained in accordance with the vendor agreement, FERPA, and the College's records retention schedule. The service is prohibited by contract from selling student information or using student information for advertising or marketing.

Students with approved accommodations are provided appropriate alternatives or adjustments through the College's established accommodation process, and accommodation records are treated as confidential.

Stillman College bears the full cost of examination proctoring. Students are charged no fee for proctoring or for any other method of student identity verification.

Video Conferencing and Recorded Course Sessions

Online courses may use video conferencing platforms for live instruction, meetings, advising, presentations, or student support.

If a class session or meeting is recorded, students shall be notified that recording will occur. Recordings may include student names, voices, images, chat messages, shared screens, or participation.

Course recordings are intended for instructional use only and may not be downloaded, copied, shared, posted, or distributed without authorization. Access to recordings shall be limited to individuals with a legitimate educational interest.

Third-Party Vendors and Educational Technology

Stillman College may use approved third-party vendors to support online learning, student services, assessment, communication, security, or administrative functions.

The College requires “may be required to complete” that third-party vendors:

- Protect student information in accordance with FERPA and applicable laws;
- Use student data only for authorized institutional purposes;
- Maintain appropriate security safeguards;
- Do not sell student information;
- Do not use student information for unauthorized advertising or marketing;
- Limit access to student information to authorized vendor personnel; and
- Return, delete, or securely dispose of student data as required by contract or institutional procedure.

Faculty and staff should use only College-approved technologies when collecting, storing, or transmitting student information.

Data Security Safeguards

Stillman College maintains administrative, technical, and physical safeguards to protect student information.

These safeguards include:

- Secure login portals;
- Password-protected access;
- Two-step verification;
- Role-based access controls;
- Single sign-on;
- Encryption where appropriate;
- Firewalls and network monitoring;
- Secure servers and data storage;
- Backup and recovery procedures;

- Software updates and security patching;
- Access logging and monitoring;
- Employee training; and
- Incident response procedures.

Faculty and Staff Responsibilities

Faculty and staff are responsible for protecting the privacy of online students and maintaining the confidentiality of student records.

Faculty and staff must:

- Access student information only for legitimate educational or job-related purposes;
- Use College-approved systems for communicating grades, feedback, and student information;
- Avoid transmitting sensitive student information through unsecured methods;
- Protect login credentials and devices used to access student records;
- Report suspected unauthorized access or data breaches;
- Follow FERPA and institutional privacy policies; and
- Complete any required privacy, cybersecurity, or FERPA training.

Student Responsibilities

Students are responsible for protecting their personal information and maintaining the integrity of their online learning accounts.

Students must:

- Safeguard their SID, username, password, and authentication information;
- Use only their own credentials to access College systems;
- Log out of College systems when using shared or public devices;
- Immediately report suspected unauthorized account access;
- Refrain from sharing course recordings, materials, or student information without authorization;
- Comply with the Academic Dishonesty Policy and Code of Conduct;
- Use College-approved platforms for course-related activities; and
- Maintain current contact information with the College.

Records Retention and Disposal

Student records, LMS data, course records, assessment records, and related electronic information will be retained in accordance with the College's records retention schedule, FERPA requirements, accreditation requirements, and applicable laws.

Records that are no longer required shall be securely disposed of, deleted, archived, or destroyed in accordance with College procedures and applicable legal requirements.

Privacy Incident and Breach Reporting

Any suspected or confirmed unauthorized access, disclosure, loss, misuse, or compromise of student information must be reported promptly to the Information Technology Department and/or the appropriate College administrator.

The College will review reported incidents and take appropriate action, which may include:

- Investigating the incident;
- Securing affected systems or accounts;
- Notifying affected individuals when required;
- Implementing corrective measures;
- Documenting the incident; and
- Taking disciplinary or contractual action when appropriate.

Accessibility and Accommodations

Stillman College is committed to ensuring that privacy protections are maintained when providing accessibility services or academic accommodations to online students.

Disability-related information and accommodation records will be treated as confidential and shared only with individuals who have a legitimate educational or administrative need to know.

Training and Awareness

Stillman College provides training and guidance to faculty, staff, and students regarding FERPA, cybersecurity, identity verification, LMS access, and online privacy practices.

Faculty and staff with access to student records must complete privacy, FERPA, or cybersecurity training as determined by the College.

Publication of Policy and Procedure

The Privacy Protection for Online Students Policy and Procedures are publicly available on the College's website and are also included in the Student Handbook to ensure that students have convenient access to information regarding the protection of their privacy and personal information.

Students are also notified in writing at the time of registration or enrollment that Stillman College charges no additional fees or projected charges for the verification of student identity.

Compliance

Compliance with this policy is mandatory. Failure to comply with or adhere to the policy may result in disciplinary action, up to and including suspension or expulsion from the College.

Employees who fail to comply with this policy may be subject to disciplinary action in accordance with applicable College policies and procedures.

Vendors or third-party service providers who fail to comply with privacy or security requirements may be subject to contract review, restriction, termination, or other appropriate action.

Policy Review

The Office of Information Technology, alongside Academic Affairs and the Office of the Registrar, conducts an annual review of this policy or updates it immediately following significant changes to online learning systems, identity verification, or legal mandates. Any revisions—ensuring ongoing compliance with technical, legal, institutional, and accreditation standards—are subject to review by the Academic Affairs Committee and approval by the President. Official effective dates and historical revisions are stored in the Stillman College Archives and the Office of Institutional Effectiveness and Research.