MERCER UNIVERSITY

UNIVERSITY POLICIES

Title:	Protecting the Privacy of Students Enrolled in Distance Education Courses and Programs
Effective Date:	February 1, 2026
Issuing Authority:	Provost
Policy Contact:	Vice Provost provost@mercer.edu, 478-301-2110

Purpose

This document contains the procedure for protecting the privacy of students enrolled in distance education courses and programs.

Scope

This procedure applies to all University distance education courses and programs, all students enrolled in distance education with the institution, and all University employees.

Exclusions

Mercer University does not deliver courses or programs by correspondence education, as defined in the 2024 SACSCOC Resource Manual for the Principles of Accreditation.

Definitions

As used in this procedure, the following term(s) have the meaning specified below:

> **Distance Education:** Mercer University adopts the SACSCOC definition of distance education which states, "In conjunction with the federal definition, SACSCOC defines distance education as a formal educational process in which the majority (50% or more) of the instruction (interaction between students and instructors and among students) in a course occurs when students and instructors are not in the same place. Instruction may be synchronous or asynchronous." [The 2024 SACSCOC Resource Manual for the Principles of Accreditation]

Policy Statement

Mercer University protects the privacy of students enrolled in distance education courses and programs. To accomplish this, University employees and students must comply with all applicable policies and procedures.

Authenticating the Identity of Distance Learning Students

Each student enrolled in a distance education course is assigned a secure login and password that must be used to register for and to access the distance education course. Specific course

and student information are not available to any outside users. For security purposes, Mercer University enforces a complex password requirement.

Computer accounts, user identifications, passwords, and other types of access authorization are assigned to individual users and must not be written down, posted, or shared with others. All Authorized Users are responsible for any use of their assigned individual account(s). Authorized Users may not run or otherwise configure software or hardware to intentionally allow access to an account by unauthorized individuals. Any attempt to use or hack another person's computer account is a violation of University policy and may also be a violation of federal, state, or local laws. Violations of this policy may result in immediate termination of access to Mercer's computer and network resources, referral to the appropriate University authority for review and adjudication, and criminal or civil prosecution.

Procedure

Secure Student Access to Distance Education Courses

- Students enrolled in Mercer University distance education access instructional systems using credentials issued by the institution.
- Multi-factor authentication is required for access to the University's learning management system—Canvas—and other University-supported instructional technologies.
- Access to distance learning course sites, instructional materials, assessments, and live or recorded web meetings are secured within Canvas.
- Access to online course sites, instructional materials, and assessments is restricted to:
  - Students officially enrolled in the course
  - Assigned instructors
  - Authorized university personnel
- Session duration in Canvas is time-limited with redirection to the sign-on page to protect student privacy.
- Access is secured through Active Directory Federation Services (ADFS) Single Sign-On's authentication.

Deliver Distance Education Through Secure, University-Supported Platforms

- Faculty teaching distance education courses use University-supported platforms that require multi-factor authentication to:
  - Communicate with students
  - Post course materials
  - Deliver assessments
  - Collect and evaluate student work
  - Post grades
- Employees use University-approved systems for official communication related to student progress, feedback, and grading.
- Employees do not post or share student educational records or personally identifiable

information in publicly accessible environments.
- Student access is limited to their own personal information and course submissions within University-supported platforms.

Maintain Confidentiality of Student Work, Grades, and Academic Records

- Employees are responsible for ensuring that:
  - Student work, grades, and feedback are accessible only to the individual student and authorized personnel.
  - Students do not have access to other students' submissions, grades, or academic records.
- Employees do not share student usernames, passwords, grades, or academic information with unauthorized individuals.
- Employees must disclose the business purpose for accessing student records, attest to understanding associated university rules, commit to maintaining confidentiality and security of student records, and receive approval from appropriate University administrators before receiving access to U.S. Family Educational Rights and Privacy Act (FERPA) protected information.
- Students may authorize or restrict access to academic or financial information, and employees are notified of the authorizations or restrictions when accessing student records.
- University employees are required to undergo cybersecurity training at the time of hire and at least annually thereafter.
- Students are prohibited from sharing their University login credentials with others.

Manage Recording of Distance Education Instruction

- When instructional sessions or course activities are recorded, faculty inform students through the syllabus, Canvas, or course communications.
- Recorded instructional content is stored within University-supported systems.
- Access to recordings is limited to:
  - Students enrolled in the course
  - Authorized University personnel
- Recordings are used solely for instructional purposes and are not distributed outside the course without appropriate authorization.
- Students may not record, reproduce, or share instructional sessions or course content without permission.

Protect Student Privacy During Online Assessments

- Distance learning assessments are conducted either within the secure learning management system or via proctored services.
  - The learning management system restricts a student's access to their instance of examinations and submissions.

- Proctored services require presentation of legal and University-issued documentation of identity and that the student completes any submission in isolation.
- When proctored services are required, these services are used only for assessment purposes.
- Specific assessment practices may vary by course or program. Students are informed of assessment requirements in advance.

Addressing Privacy Questions and Concerns

- Student concerns related to privacy in distance education courses or programs are addressed through University grievance policies, including additional avenues for distance education students, as published in the Mercer University Student Handbook.
- Distance learning students have access to the University IT Help Desk for any technical issues involving student account information. The University IT Help Desk verifies student identity prior to service with the last four digits of their student identification number and their date of birth.
- All University web-based applications and sites that collect personally identifiable information for distance learning students are secured, encrypted websites using standard Secure Socket Layer (SSL) certificates.

Additional Resources

The following Mercer University policies provide institutional requirements for compliance related to this procedure:

1. Academic Integrity Policy: https://policies.mercer.edu/academic-integrity/
2. Cybersecurity Awareness Program Policy: https://policies.mercer.edu/cybersecurity-awareness-program/
3. Data Security Policy: https://policies.mercer.edu/data-security/
4. Email Access and Use Policy: https://policies.mercer.edu/email-access-and-use/
5. Family Educational Rights and Privacy Act (FERPA) Policy: https://policies.mercer.edu/family-educational-rights-and-privacy-act-ferpa/
6. Information Technology Access and Use Policy: https://policies.mercer.edu/information-technology-access-and-use/
7. Security of Student Records Held in Offices Policy: https://policies.mercer.edu/security-of-student-records-held-in-offices/
8. Student Grievance Policies:
    a. Academic Grievance and Appeal Policy: https://policies.mercer.edu/academic-grievance-and-appeal/
    b. Non-Academic Grievance and Appeal Policy: https://policies.mercer.edu/non-academic-grievance-and-appeal/
    c. Student Handbook - Grievance Policies and Procedures: https://provost.mercer.edu/resources/handbooks/student-handbooks/

History

Approved by the Provost: February 1, 2026