

Title: Student Authentication	Policy No: 3.18
Category: Academic Administrative Processes	Effective: Fall 2015

Policy Statement: The University of Central Oklahoma must operate in compliance with the provisions of the United States Federal Higher Education Opportunity Act (HEOA), Public Law 110-315 concerning the verification of student identities. This policy applies to all courses and programs offered by the University of Central Oklahoma, beginning with the application for admission and continuing through to a student’s graduation, transfer, or withdrawal from study.

Background: It is a national challenge for instructors to know if the student enrolled in a distance education class is the actual person who is logging in and turning in his/her own work. The Higher Education Opportunity Act of 2008 requires the verification of students who participate in courses or programs provided through distance (online, hybrid, interactive video course) or correspondence [self-paced online course (SPOC)] education.

Purpose: Student authentication procedures assist and ensure that the student who registers for a distance education course or program is the same student who participates in and completes the course or program and receives academic credit as appropriate.

Responsibilities:

Authentication Methods

When faculty will not be physically present during the course to verify student identities, at least one of the following methods must be used:

Secure Login and Password: Each student has their own assigned UCONNECT Username and student-generated password to log into university systems.

Proctored Examinations: The University’s Proctoring Policy and Procedure should be used as a guiding reference for proctored examinations. (See Policy 3.19)

New or Emerging Technologies: Third party vendors that provide robust identity verification software services (e.g., services similar to those used in the financial sector) could be used as an option by the Colleges.

Pedagogical and Related Practices: Online instructors have a responsibility to identify changes in students. Examples of changes could be a sudden change in academic performance, change in writing style, as well as odd statements by students in discussions or email. To aid in spotting such changes, instructors should use more than one kind of assessment type and ask students to share important ideas learned from references.

All methods of verifying student identity must protect the privacy of student information. Personally identifiable information collected by the university may be used, at the discretion of the institution, as the basis for identity verification. For instance, a student requesting that their learning system password be reset may be asked to provide two or more pieces of information for comparison with data on file, or to come to the University in person with a photo ID for verification.

Security for University System Users

All users of university systems are responsible for maintaining the security of usernames, passwords and any other access credentials assigned, in accordance with UCO's information technology security policies. Access passwords may not be shared or given to anyone other than the user to whom they were assigned to for any reason.

Student users are responsible for any and all uses of their account. Users are responsible for changing passwords periodically to maintain security. Users are held responsible for knowledge of the information contained within the most recent University Catalog as well as the Student Handbook. Failure to read university guidelines, requirements and regulations will not exempt users from responsibility. Refer to the [UCO Code of Student Conduct](#) for disciplinary actions when not complying with policy. Students are responsible for providing accurate and true information in any identity verification process.

Faculty/Staff/Administrator Responsibilities

Faculty teaching courses have the primary responsibility for ensuring that their courses comply with the provisions of this policy. The Office of Academic Affairs shall be responsible for evaluating, selecting, and implementing any new technologies being used to verify student identity. In doing so Academic Affairs should consult and cooperate with appropriate university stakeholders including Information Technology and the Center for eLearning and Customized Education.

Because technology and personal accountability may not verify identity absolutely or ensure academic integrity completely, faculty are encouraged, when feasible and pedagogically sound, to design courses that employ assignments and evaluations unique to the course and that support academic integrity.

Deans and institute directors are responsible for ensuring that faculty are aware of this policy and comply with its provisions. They are also responsible for ensuring that academic awards and degree programs within their units comply with the provisions of this policy.

The Office of Academic Affairs is responsible for ensuring university-wide compliance with the provisions of this policy and that deans and institute directors are informed of any changes in a timely fashion. The Office of Academic Affairs is also responsible for coordinating and promoting efficient use of university resources and services, and for ensuring that university level processes (e.g., admissions or registration) also remain in compliance with this policy.

Notification of projected additional student charges associated with the verification of student identity will be posted on UCO's website under the "Financial Disclosure/Enrollment Costs" page located here (<http://www.uco.edu/em/registrar/tuitionandfees.asp>).

Compliance

In accordance with the responsibilities outlined above, deans and institute directors are expected to ensure that all faculty and staff within their units remain in compliance with this policy. The University of Central Oklahoma should have in place appropriate policies to promote the

academic integrity of its courses. Those policies should be widely disseminated throughout the university.

The university provides faculty with training to use pedagogical approaches and technology to promote academic integrity. Additionally, the university provides information to students regarding not sharing passwords and being held accountable for academic integrity.

Frequency of Review and Update

This policy will be reviewed annually by the Office of Academic Affairs for continued alignment with the appropriate federal regulations and policies and revised as necessary.

Implementation Date: Fall Semester 2015

Related Procedures:

Coordinating Offices: Center for eLearning and Customized Education, Testing Services, and Academic Affairs

Point-of-Contact for Academic Affairs: Executive Director for Policy and Curriculum

Academic VP Signature: _____ Date: _____

Policy approved by the Vice President/Provost for Academic Affairs on June 10, 2015