Federal Compliance

Verification of Student Identity in Online Learning

In accordance with the Higher Education Opportunity Act (HEOA)(Public Law 110-315), Federal Requirement 34 CFR §602.17(g), and HLC Policy Number FDCR.A.10.050, institutions offering distance or correspondence education must have processes to establish that the student who registers in such courses is the same student who participates in and receives academic credit. McKendree University offers online courses, which fall under the definition of distance education, and this policy applies to all programs beginning with the application for admission and continuing through a student's final day at the institution.

Practices for Verification of Student Identity

Introduction

The following institutional practices are identified by the aforementioned HEOA/HLC guidelines as acceptable practices for verifying student identity:

- A secure login and passcode
- Proctored examinations
- New or other technologies and practices

Students must be informed at the time of registration and/or enrollment of any projected additional student charges associated with verification of student identity. Methods used also must have reasonable safeguards to protect student privacy.

Fees

There are no student fees relating to verification of student identity.

Network User Account

During the application and admission process, student identity is vetted in accordance with standard practices. Upon matriculation, each student receives a unique and secure McKendree University network user account. This network user account allows the student to authenticate into nearly all McKendree University systems, including the learning management system, email, student portal, grades, etc. All systems are secured in accordance with industry best practices.

A network user account serves as the secure login and passcode for every McKendree University student. Before a network user account can be used to access university systems, a student must first activate the account using a designated activation system. Students log into this activation system with unique identifying information (see Information Technology Account Management page). As part of the activation process, each student must read and accept the terms of the Authorized User agreement, which explains the terms of use of the network user account, including:

- Network user account credentials may not be shared or given to anyone other than the user to whom they were assigned
- User responsibilities for keeping account credentials secure
- Disciplinary action for violating terms of the agreement

Network user account credentials are managed by authorized users at accounts.mckendree.edu, a secure online account management system. This management system allows for self-service of network user account functions such as password resets, setting up security questions, and unlocking of accounts.

Security features of network user accounts include locking of the account after multiple unsuccessful login attempts (i.e. incorrect password), security questions set up by the user, and available two-factor authentication.

These policies and features of network user accounts, while not absolute in verification of student identity, offer reasonable assurance that the appropriate user is authenticating to university systems.

Proctored Examinations

Technology for proctoring web-based examinations is available for instructors to use in any course – including all online courses – through McKendree's learning management system. Certain programs and/or courses require the use of proctoring for online examinations. Proctoring technology includes:

Browser lockdown

Exams taken within the learning management system environment can require the use of browser lockdown technology. Such technology ensures the device used for taking an online exam prohibits use of programs and features outside of the testing environment.

Exam monitor

Exams administered within the learning management system environment can require the use of monitoring technology, which facilitates visual identification of the student, presentation of ID cards, inspection of local testing environment, video recording of exam session, and automatic flagging of suspicious behavior during the exam. Instructors can choose to implement any/all of these features.

Other technologies or practices

In addition to the measures stated thus far, other technologies, practices, and policies aid in the verification of student identity.

Population of information from data system

University systems that facilitate user access to course registration, course delivery, internet communication, financial aid, billing, and other services are populated directly and automatically by the data system. Accessing these systems requires a student to authenticate using their network user account.

Learning management system usage policies

Course sections and course rosters are populated automatically based on academic record information in the data system, with the exception of non-credit courses used for information or technology administrative purposes. Users may not create their own courses or accounts, ensuring that only those with valid network user accounts may access the system and that users may only access resources designated to their user accounts.

Audio/Visual identification

In the learning management system, the email system, and other applicable systems, students can associate a photo with their account, allowing for visual identification of the student. Technology for live audio and/or visual communication, which can be helpful in verifying student identity, is also available for faculty, staff, and students.

Other learning management system features

The learning management system environment features further tools that can be used by instructors to help ensure that students are performing their own work. Plagiarism detection tools are available to help determine the identity of those who submit the work. Exams can require a passcode as offered to students by the instructor. Network IP restrictions can also be utilized to restrict access to the system.

Privacy

McKendree University is compliant with the provisions of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, which protects the privacy of student educational records. Further information is available in the Student Data Privacy Policy.