wcet
Partners for change.
Technologies in practice.
Advances in education.

Academic Integrity and Student Authentication

Sponsored by the WCET Study Group on Academic Integrity and Student Authentication.

March 2009 Message from Study Group Chair, Rhonda Epper."We hope this WCET update on the federal rulemaking process and our own work to date on the issue of student authentication in distance education helps to guide your own institution's thinking during this interim period before Dept. of Education guidelines are determined...."

Introduction

Higher Education Opportunity Act of 2008

Resources

Institutional Practices

Introduction

Academic Integrity and Student Authentication

A perennial question asked of distance and online educators is whether student cheating occurs more easily or frequently in an online setting. There is little research to support claims that online learners are at a higher risk for cheating, or that they behave any differently from traditional students when it comes to academic honesty. And yet, many educators and policy leaders believe there is a need to more carefully monitor student authenticity in an online class setting.

Over the past decade, concerns about the lack of face-to-face faculty-student interactions have forced online and distance education providers to continuously examine their programs and develop sophisticated approaches to ensure the integrity of their academic programs. In fact, online and distance educators perhaps have done more to align pedagogy, assessments, and learning objectives than many traditional postsecondary programs.

Strategies used by distance education providers to ensure academic integrity and student authenticity fall into two general categories: prevention and compliance. These approaches are discussed in greater detail in the WCET briefing paper. "Prevention" approaches include the use of multiple assessment techniques, greater reliance on discussion and written work, use of "test banks," timed test delivery, and communicating behavior expectations to students. "Compliance" approaches include secure login credentials, plagiarism detection software, browser lock-down systems, physical proctoring for exams, and remote proctoring.

But Can The Student Still Cheat? It is important to note that even if an institution carefully implements a combination of the approaches outlined above, a student who is determined to cheat may still succeed in doing so. Little research exists that compares the cheating behaviors of on-campus and online students. There is, however, some research into faculty opinions about the cheating behaviors of online students compared to on-campus students. Faculty members who have experience teaching online see no difference between the two methodologies when it comes to student cheating.

In 2008, WCET established a Study Group on Academic Integrity and Student Verification in Online Learning to create a body of expertise and shared knowledge about strategies, resources, and good practices. The Study Group has sponsored a webcast, conference presentation, briefing paper, survey, draft set of good practices, and has served in an informal advisory role to negotiators participating in the U.S. DOE negotiated rulemaking process.

Source: WCET Briefing Paper, February 2008

The Higher Education Opportunity Act of 2008

The Higher Education Opportunity Act of 2008, Public Law 110-315, was enacted August 14, 2008. Title IV, Part H of the law concerns Recognition of Accrediting Agencies. It includes a new obligation on accrediting agencies to require "an institution that offers distance education to have processes through which the institution establishes that the student who registers in a distance education course or program is the same student who participates in and completes the program and receives the academic credit."

The Conference Report that accompanied the HEOA legislation provides guidance to institutions and accreditors in the interim to allow for the U.S. Department of Education's rulemaking process to develop proposed regulations to implement the HEOA. Until the U.S. DOE announces new guidelines, institutions may be guided by the following Conference Report language:

"The Conferees expect institutions that offer distance education to have security mechanisms in place, such as identification numbers or other pass code information required to be used each time the student participates in class time or coursework on-line. As new identification technologies are developed and become more sophisticated, less expensive and more mainstream, the Conferees anticipate that accrediting agencies or associations and institutions will consider their use in the future. The Conferees do not intend that institutions use or rely on any technology that interferes with the privacy of the student and expect that students' privacy will be protected with whichever method the institutions choose to utilize."

In February 2009, the U.S. Department of Education announced the establishment of the five committees, with Team III assigned to address issues related to accreditation, including the provision about the authentication of distance education students. Information about the rulemaking process and the committee is available on the U.S. DOE website [http://www.ed.gov/policy/highered/leg/hea08/index.html].

Academic Integrity and Student Authentication - Resources

Institutional Policies/Practices and Course Design Strategies to Promote Academic Integrity in Online Education
[http://wiche.edu/attachment_library/Student_Authentication/Academic_Integrity_Strategies_Feb09_Draft.pdf]
Based on the "Best Practices for Electronically Offered Degree and Certificate Programs" adopted by the regional accrediting associations, WCET's study group drafted a companion set of good practices to promote academic integrity. This work is still in progress.

WCET 2008 Conference Presentation
The WCET Study Group on Academic Integrity and Student Authentication sponsored a presentation at WCET's November 2008 annual conference with updates on the federal rulemaking process concerning the HEOA. (See slide presentations from Epper [http://wiche.edu/attachment_library/Student_Authentication/Survey_Summary.pdf], Beno [http://wiche.edu/attachment_library/conference_presentations/whats_around_the_corner_beno.pdf], Gilcher [http://wiche.edu/attachment_library/conference_presentations/whats_around_the_corner_gilcher.pdf], McNabb [http://wiche.edu/attachment_library/conference_presentations/whats_around_the_corner_mcnabb.pdf])

WCET Webcast 10-01-08 Slides [http://www.wcet.info/2.0/index.php?q=node/973]
On 10-01-08, WCET sponsored the webcast, "What's Around the Corner? Clarifying Student Authentication in the Higher Education Opportunity Act of 2008.

Are Your Online Students Really the Ones Registered for the Course? A WCET Briefing Paper [http://wiche.edu/attachment_library/Briefing_Paper_Feb_2008.pdf]
A WCET Briefing Paper, published February 2008, on the pending federal legislation concerning the authentication of distance education students.

Fundamental Values Project [http://www.wcet.info/2.0/index.php?q=node/1216]
The Center for Academic Integrity's Fundamental Values Project created a definition of academic integrity and identified the key elements of a successful academic integrity program.

WCET Executive Briefing August 2005
[http://wiche.edu/attachment_library/Student_Authentication/Executive_Briefing0805.pdf]
Article by Sally Johnstone about the proposed student authentication provision in 2005 and institutional strategies to promote academic honesty.

Student Authentication - Institutional Practices

Summary of WCET Survey.

Summary of August 2008 WCET survey
[http://wiche.edu/attachment_library/Student_Authentication/Survey_Summary.pdf] of institutional policies and practices used by online and distance education programs to promote academic integrity.

Examples of Institutional Practices and Policies

Example #1: LDAP (Lightweight Directory Access Protocol) is an industry-standard authentication program that is used by students accessing Web course and other secure Internet information including e-mail. In addition, all students agree to an acceptable use policy that prohibits sharing logon and password information. Penalties for academic dishonesty are clear and widely disseminated in syllabi and the Student Handbook.

Example #2: For student authentication, we use secure sign-on - first, because our current system works well and is consistent with best practice, and second, because the alternatives have serious drawbacks. For example, many states consider proctoring as physical presence. Also, technologies such as biometrics and webcam monitoring are prohibitively expensive and could be considered overkill for this kind of application.

Example #3: If you are teaching or working within [name of institution and LMS], please keep in mind that your secure login credentials are an important defense against academic dishonesty. We recommend the use of "strong passwords," which should:

- have a minimum length of eight characters
- be comprised of a combination of alpha, numeric, or special characters
- be treated as confidential information
- be changed immediately if the security of the password is in doubt

When creating a strong password, you should NOT include any of the following:

- your name, nickname, birthday, interests, or information known or easy to learn about you
- your address, street name, phone number, town, or city

- names of your family, friends, pets, or co-workers
- your social security, driver's license, license plate, or other series of assigned numbers or letters
- the name or abbreviation of your school, department, or area of study
- your school mascot, colors, or slogans
- word or number patterns such as aaabbb, zyxwvut, 123456, or 123321
- slang words, obscenities, popular phrases, acronyms, or jargon
- words that appear in an English or foreign dictionary
- passwords selected for personal use or commonly used on public web sites
- the reverse of any of the above

Example #4: Many campuses have "acceptable use" policies for students, faculty and staff that address areas such as network use consistent with institutional mission, copyright compliance, misuse of computing resources (e.g, sharing institutional account passwords) and consequences of possible loss of network privileges and/or disciplinary action.