Safeguarding Academic Integrity in the Age of Agentic AI

A White Paper from the California Virtual Campus (CVC)

November 2025

Overview

The rapid emergence of *agentic artificial intelligence (Agentic AI)*, or systems capable of autonomously performing digital tasks, presents a new and urgent challenge for systems of higher education, including the California Community Colleges (CCC). Unlike traditional AI text generators, Agentic AI systems such as Perplexity Comet, ChatGPT Agents, and ManusAI can log into web platforms, navigate interfaces, and complete actions that mimic authentic user behavior. *This means that they may be used by students to log into Canvas, search for required assignments, assessments or tasks, and complete these on behalf of the student autonomously.*

Although Agentic AI presents significant concerns about security and privacy, disabling firewalls, and leaking sensitive data in student portals and student information systems, this white paper focuses on academic integrity in fully online courses and the California Community College's efforts to respond to these growing concerns.

The Problem: Agentic AI and the Integrity of Learning Environments

CCC faculty report that these tools can log in to Canvas and complete quizzes, discussions, and assignments on behalf of students. This behavior threatens the integrity of online learning, undermines authentic assessment and creates serious implications for equity, accreditation, and public trust. Specifically, Agentic AI, under most circumstances, can do the following:

- Autonomously log into Canvas using student credentials;
- Navigate course shells, view materials, and complete assignments and quizzes;
- Submit work that appears mostly indistinguishable from human activity;
- Operate undetected because they mask their digital identity (e.g., by mimicking standard browser user agents like Chrome).

These tools effectively enable *unauthorized participation in coursework*, allowing users to delegate learning to machines. The result is an erosion of trust between students and instructors, compromised assessment validity, and an uneven playing field for students acting with integrity. The Modern Language Association, along with several other organizations have called for direct engagement with both faculty and vendor partners to cooperate in finding solutions.

Colleges have also noted that current Canvas tools and institutional detection mechanisms are not equipped to identify or block these automated activities. While some colleges have discussed reverting to in-person proctoring or handwritten exams, such shifts could risk accessibility and disproportionately impact working adult learners, students with disabilities, and those reliant on fully online learning for equitable access.

Systemwide Response and Coordination

It should be noted that no single technical solution currently exists to address the use of Agentic AI in all contexts. Moreover, recognizing that no single institution can address this alone, the following coordinated response that includes:

1. Direct Engagement with Instructure (Canvas)

Instructure leadership have been apprised of this concern and are currently grappling with it; they have issued a brief statement about AI and Academic Honesty. CVC leadership has elevated the issue to Instructure's executive team, urging:

- The development of agent detection and blocking tools at the LMS level;
- Transparent communication to institutions on technical roadmaps related to AI and integrity protections;
- Vendor partnerships between Instructure and other AI technology vendors to prevent the use of certain access points in Canvas.

2. Collaboration with Technology Partners

The CCCCO is piloting solutions with cybersecurity partners to test layered defense strategies, including:

- Advanced detection and network-level restrictions to prevent agentic browsers from accessing Canvas via institutional domains.
- Single Sign-On (SSO) enforcement with multifactor authentication (MFA) for student access;
- Use of lockdown browsers to prevent browser extensions and other activities.

3. Systemwide Collaboration and Professional Development Opportunities

- CVC@ONE has been offering systemwide webinars on a variety of topics around Agentic AI, and will continue to do so. You may watch archived recordings of these on the CVC@ONE YouTube channel
- The Common Course Management System (CCMS) committee, which has representation from a broad range of constituents, offers monthly updates on new Instructure releases and mitigation strategies, as we learn about them. Contact support@cvc.edu to find out who your representative is on this committee.
- Instructure offers monthly updates for our system, which will also include any updates to Canvas features. Contact your Canvas CSM for an invitation and link to these: knichols@instructure.com or gteixeira@instructure.com.

Recommendations for Local Colleges and Districts

Until system-level protections are available and fully implemented, colleges can take meaningful local steps to mitigate risks and strengthen academic integrity:

1. Adopt and/or contribute to systemwide best practices for policy and academic integrity frameworks:

    - Engage the Academic Senate for California Community Colleges (ASCCC), California Community College Distance Education Coordinators' Organization (CCCDECO), and professional development networks to clarify expectations for AI use statements and academic integrity policies;
    - Raise the issue with local academic senates, distance education, and curriculum committees;
    - Ensure your academic honesty policies explicitly address AI agents and digital impersonation, both at the institution-level and on course syllabi.

2. Support Faculty in adopting new assessment strategies:

    - Consider Project-Based Learning (PBL), authentic assessments, and other pedagogical adaptations that maintain authentic learning. While technical measures are critical, faculty can also emphasize process-based assignments, interactive learning, and personalized assessments that are more resistant to automation;
    - Provide training and communication resources for faculty and students about responsible AI use;
    - Have your college's Distance Education (DE) coordinator access and add to shared resources through the CCCDECO such as collecting examples of systemwide policies.

3. Engage IT and LMS administrators:

    - Limit API tokens in Canvas as much as possible; the current recommendation is to eliminate the use of student tokens altogether and only enable them when absolutely necessary (and limit them within that timeframe);
    - Review local Single Sign-On (SSO), Multi-Factor Authentication (MFA), and password policies for vulnerabilities;
    - Utilize tools such as Instructure's *Intelligent Insights* to examine student online behavior to better understand the impact of agentic AI (for example patterns of activity, time on assessments, etc.).

Conclusion

Agentic AI poses a direct challenge to the integrity of digital learning environments, but it also offers an opportunity for systemwide innovation and cooperation. Through our joint engagement and collaboration, the California Community Colleges are taking a leadership role nationally in defining ethical, secure, human-centered, and student-centered uses of AI in education.