

Academic Platforms & Your Privacy

Briefing for Instructional Designers

Learning Management Systems (LMSs) and other educational-technology platforms—such as proctoring software, etextbooks, and plagiarism detection—are heavily used in higher education. These tools can pose significant privacy and surveillance risks to our students.^{1,2} Evaluating what data these platforms collect on students,³ what data we ourselves collect and use, how to limit data collection and retention, and when to take corrective action or use alternative platforms are all actions that can safeguard student privacy.

Key Privacy Concerns

- Student data is collected by educational technology platforms, often without student input or awareness and often without vendors clearly communicating what information is being collected and how it may be used.⁴
- Platforms are required for many courses, so students cannot avoid using them.⁵
- Instructors are not always familiar with privacy risks of educational technologies or strategies for mitigating them.⁶
- Instructional designers should seek to understand data privacy concerns and identify best practices and paths forward.⁷
- Instructional designers rarely help acquire campus educational technologies. As such, they may not have input into the underlying technologies' permissions, restrictions, or other privacy practices. However, they can educate themselves and use best practices in their design.⁸

What You Can Do

- Connect with the library. Library workers are experienced with resource licensing, university acquisitions processes, ILS integrations, and vendor privacy issues.
- Consider privacy-protecting alternatives for problematic tools. For instance, lower-risk institutionally-hosted options may be available for document collaboration.⁹
- Advocate and ask questions about privacy protection in meetings and consultations.
- Determine and reflect on how you are supporting and promoting student education and agency on personal data collection, governance, and usage.¹⁰
- Discuss with instructors the ethical implications of monitoring student activity within an LMS. What settings can be changed or disabled? What data must be present to appropriately grade students? Only gather data the instructor needs.
- Inform instructors that research based on identifiable student data should go through human-subjects review¹¹ and follow all institution-level data policies. Carefully consider any personal data that may be shared with research partners outside the institution.
- Discuss with instructors the actual need for the specific tool they want to use in their course, especially for highly privacy-concerning tools such as exam-proctoring software.¹² Are there better alternatives that are more ethical and effective?

- Following the completion of a course, remove student data from an LMS. Create and follow data retention schedules.

References

1. [Privacy considerations in higher education online learning](#) by Chris Sadler.
2. [Platforms like Canvas play fast and loose with students' data](#) by Britt Paris, Rebecca Reynolds, and Catherine McGowan.
3. [The 'Textbook' That Reads You](#) by Taylor Swaak.
4. [Paying Twice to Learn: How Higher Education Students May be Forced to Sacrifice Privacy for Digital Learning Tools](#) by Ariel Fox Johnson.
5. [He wanted privacy. His college gave him none](#) by Tara García Mathewson.
6. [The case for including data privacy and data ethics in educator preparation programs](#) by Ellen D. Mandinach and Juliana Cotto.
7. [Beyond identifying privacy issues in e-learning settings – Implications for instructional designers](#) by Hui-Lien Chou and Chao-Hsiu Chen.
8. [A quick skim of legal considerations in instructional design](#) by Shalin Hai-Jew.
9. [Privacy](#) by the Cornell Center for Teaching Innovation.
10. [Education before regulation: Empowering students to question their data privacy](#) by Autumm Caines and Erin Glass.
11. [Does my research require IRB review?](#) By UCSF Human Research Protection Program.
12. [On the necessity \(or lack thereof\) of digital proctoring: Drawbacks, perceptions, and alternatives](#) by Alex Duncan and David Joyner.

About the Campus Briefings on Privacy & Academic Platforms

- This briefing was authored by the Resource Library Working Group of SPARC's Privacy & Surveillance Community of Practice which seeks to ensure privacy is fundamental to the future of research & education.
- See additional briefings and a glossary of terms at sparcopen.org/our-work/privacy-briefing-documents