Policy as an Enabler of Student Engagement

Today’s educators are faced with a multitude of tools (e.g., collaborative workspaces, chat rooms, blogs, wikis, and podcast/video sites) that offer new potential for engaging students in learning. When such tools are institutionally provided, instructors can be confident that relevant policy issues have been addressed. But many instructors also want to use third-party hosted tools that are not yet offered by their institution or that are impractical or impossible for the institution to implement or purchase. Institutions struggle with how to appropriately manage the review of these tools for compliance with policy and applicable law concerning data privacy, security, and protection of intellectual property rights, especially given the exploding use of these tools and the typically limited number of knowledgeable staff to conduct reviews.

So if an institution can’t keep up with all of these tools, what can it do? Some higher education institutions provide guidance for their instructors to perform reviews themselves. For example, the Indiana University Teaching Handbook includes a section titled “Use of Social Networks, Blogs, Wikis, and Other Third-Party Hosted Tools in Instruction,” which builds on an excellent and more succinct model created by the University of Wisconsin–Madison, to assist its faculty. Such detailed guidance is necessary for complicated or inventive uses of technology in instruction. But will the majority of instructors dabbling in the use of such tools spend the time needed to carefully consider all the issues outlined? Or will they glance at the length of these laundry lists and decide against dabbling at all, thus missing an opportunity to increase student engagement?

In fact, some Indiana University faculty have responded to the university’s comprehensive self-service guidance by requesting that administrative staff conduct the reviews rather than asking instructors to do so. Certainly this would be ideal, reducing duplicative efforts and better ensuring that all risks are accounted for and addressed. But this may not be feasible, especially when staffing is lean, and the time delay required for a third party to review the instructor’s plans may also introduce a barrier to faculty innovation.

Institutions may want to consider another strategy. In most cases, risks associated with the use of these tools can be minimized through the instructor’s proactive review of just the most critical risks, ensuring that student engagement can be enhanced without endangering the institution.

Just How Risky Is the Technology Tool?

IT and legal professionals tend to exhaustively identify the policy, security, privacy, and legal issues associated with a new and innovative technology, treating each issue with the same level of importance. It is true that all issues need to be identified, but not all of the issues need to be considered equally. Moreover, issues may pose different levels of risk when the technology is used for different purposes; for example, an increasing number of institutions have outsourced student e-mail but not employee e-mail.

The most common uses of such technologies in instruction today do not pose the same level of risk as would be the case if the tools were used in, for example, e-commerce, donor relations, or patient care. Keeping this in mind, and as a measured response to the faculty request regarding reviews, a team at Indiana University evaluated the issues associated with uses of “cloud” technologies, consulted instructors about how they used third-party technologies in instruction, and strived to whittle the guidance down to the minimum necessary for the majority of instructional situations. Only three directives to instructors emerged.

In most cases, risks associated with the use of these tools can be minimized through the instructor’s proactive review of just the most critical risks.

#1: Don’t put any information classified as highly sensitive into a third-party service without entering into a contract with the vendor. Institutions should have a data-classification scheme, which identifies the information requiring the very highest level of protection. If the pedagogical objectives of the course require the instructor or students to enter this type of information into the third-party system, the instructor should not use the system without working with the appropriate institutional office to contractually require the service to comply with necessary security and privacy policy, law, and regulation. Fortunately, very few instructional activities will require the use of highly sensitive data, so the vast majority of instructors can move on to the second directive.
A standard institutional copyright notice typically must be included when the content is uploaded.

If the rights are owned by the instructors or students, they should review the terms of service to ensure that they understand and are comfortable with those terms, and they should consider placing copyright notices on their content.6

Summary
In nearly all cases of using technologies to increase student engagement in learning, instructors can focus on three key risks: highly sensitive information, FERPA-protected information, and intellectual property. This leaves a small number of complex and inventive projects that will require additional scrutiny and full administrative review of the additional risks.

The policy, security, privacy, and legal issues related to using tools not hosted by an institution can be great, but providing lists of issues without a consideration of the corresponding risks associated with particular uses will cause policy to become a barrier to—rather than an enabler of—student engagement.

Notes
3. Many thanks to my colleagues Beth Cate, Associate General Counsel, and Kate Ellis, Instructional Technology Consultant.
5. The following list addresses most, if not all, sources of serious risks: Social Security numbers, credit card numbers, debit card numbers, bank account/financial account numbers, driver's license numbers, state ID card numbers, student loan information, foundation donor data, protected health information, individually identifiable health information, and passphrases/passwords, PINs, and security/access codes. Often, one of these elements needs to be accompanied by an individual's name in order to result in harm, but not always.
6. The Creative Commons license generator can help instructors and students create simple copyright notices that allow others to copy and distribute their works but that still require certain conditions, such as proper attribution. See “License Your Work,” Creative Commons, <http://creativecommons.org/ choose/>.

Merri Beth Lavagnino (mbl@iu.edu) is Chief Privacy Officer and Compliance Coordinator at Indiana University.

© 2010 Merri Beth Lavagnino. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License (http://creativecommons.org/licenses/ by-nc-sa/3.0/).