

# THINGS YOU SHOULD KNOW ABOUT... PRIVACY IN WEB 2.0 LEARNING ENVIRONMENTS

## Scenario

For several years, Dr. Schorr had been using the blog tool included in the university's LMS in his undergraduate courses in journalism. Students would write stories and post them in their blogs, and Dr. Schorr and the other students reviewed them and added comments. The students generally found the blog format valuable, and for the fall semester, Dr. Schorr wanted them to use public blogs so they could receive feedback from anyone, providing more authentic critique. Dr. Schorr evaluated several popular blogging platforms but finally decided that because many students already maintained blogs, he would allow them to use the blog tool of their choosing.

Dr. Schorr contacted the university's legal department about this project, and he was surprised to find out the extent to which public blogs might expose the institution to privacy risks. He knew, of course, that information such as Social Security or credit card numbers was sensitive, but legal counsel informed him that quite a few other kinds of information could not legally be included in the public blogs. Information in the university directory could be included, such as name and home town, but if other student data—such as class standing, major, and residence hall—found its way into the blogs, the institution could be in violation of FERPA. Dr. Schorr was advised to be extremely specific in explaining to his students what they could and could not include in their blogs and to offer them an alternative to using a public blog. He gave them the option of using the LMS blog tool and also wrote up a detailed list of items that were not allowed in the posts. Dr. Schorr also learned that he would need to be careful about the responses he left in the blogs. He had been in the habit of including detailed feedback, sometimes even saying something like “This is an ‘A’ story.” Specific grades and even evaluative comments, however, would constitute a violation of a student's privacy in a public blog.

Ultimately, despite the constraints that Dr. Schorr and the students faced in using public blogs, the feedback from the broader community was extremely valuable. Moreover, both Dr. Schorr and his students developed an acute awareness of privacy concerns and the skill to be good journalists while being sensitive to individuals' privacy.

## 1 What is it?

New media, social networking, collaboration sites, image- and video-sharing sites, wikis, and blogs offer tremendous teaching and learning opportunities to educators and students, but their use raises concerns about privacy, especially as it relates to work that students are asked to complete as part of a course. FERPA stipulates that educational institutions are responsible for ensuring the privacy of certain elements of the education record, which is defined as those records, files, documents, and other materials that contain information directly related to a student and are maintained by any employee or agent of the institution. When FERPA was enacted in 1974, the education record was limited to comments written on term papers and handwritten grade sheets submitted directly to the registrar. Higher education has moved from paper-based assignments and microfiche records or transcripts—easily kept under the physical control of the institution—to digital, often cloud-based course documents that may require protection. Today's learning environments have evolved and may now include blogs, collaborative documents, and many other electronic tools external to the institution, all of which have the potential to contain parts of the education record.

## 2 How does it work?

New learning environments often leverage Web 2.0 or cloud-based tools that offer limited or no privacy protection. When they do, those privacy settings are frequently outside the control of either the institution or the faculty member, prompting a range of questions: Should graded or optional work be posted on public sites? May peers post feedback on other students' work? Is it acceptable to leave any kind of evaluative comments on public sites containing student work? Should access to student work be limited to those in the course? The answers to these questions may vary by institution, but FERPA places the burden of ensuring the privacy of the education record on the institution. Administrators and legal counsel are sometimes unclear about the best way to protect and preserve students' privacy in open teaching and learning environments. Cloud-based technologies open new doors for pieces of education-record content to find their way past the controls that have been in place to keep that content private. For this reason, many institutions have recently developed guidelines and policies that address privacy concerns, specifically in the area of cloud-based teaching and learning.

## 3 Who's doing it?

Institutions are approaching these privacy risks in a number of ways. Pepperdine University, for example, is implementing local instances of Web 2.0 applications behind its firewall to offer students the benefits of new media within the university's secure network. Northwestern University not only provides new media tools

[more >>](#)

## THINGS YOU SHOULD KNOW ABOUT...

# PRIVACY IN WEB 2.0 LEARNING ENVIRONMENTS

shielded within the university's IT network but prohibits the use of external applications for coursework. North Carolina State University offers a FERPA Privacy Checklist for the faculty and staff that specifies guidelines and practice for online instructional environments related to FERPA obligations and compliance. Ohio State University hosts a site that features a long list of recommendations, such as educating students about the requirements for protecting information and the risks of specific tools; requiring students to use aliases when creating online accounts; restricting access to student work as much as possible within the scope of instructional goals; and not placing grades or evaluative comments on Internet sites.

### **4** Why is it significant?

Institutions are beginning to explore the connection between FERPA and student work along with their responsibilities in this area, but this represents new and vague territory for many. Course-related student work residing in the cloud might contain elements of the education record as defined by FERPA, but content stored in a cloud-based tool is generally outside the control of the institution. Although some cloud applications allow individual users to control privacy settings, students are frequently unaware of how to do so or even that they should. In this context, institutions might develop privacy guidelines and recommendations for alternatives, if any, to using cloud-based tools. Information and policy provided at the institutional level can help faculty members—who might otherwise feel they have been left to deal with privacy issues on their own—make choices about which tools to use and how to use them. Students should be educated about the risks of providing names or other identifying personal information on third-party sites that may be public. Institutions should consider how they will approach the use of these tools and how they will communicate policy, best practices, and guidelines. These efforts could include policy statements, either written or as podcasts, and resources could be made available in a central location, such as an institutional learning management system, to ensure consistency of the message.

### **5** What are the downsides?

Dealing with privacy in cloud-based instructional environments is likely new ground for many institutions and faculty members. There may be little understanding of privacy risks among the faculty and the administration, and institutional legal counsel might have little or no background addressing these issues. Given the uncertainties and risk, some legal advisors might simply advise faculty not to employ cloud-based tools in instructional environments. It's important to consider how to proceed and whom to include in the decision-making process. The difficulty is in balancing instructional innovation and student engagement—often sparked by these new media applications—with the protection of

student privacy. It will be important for institutions to engage in collective discussions to more clearly define the education record and identify the best course of action: policy, guidelines, information sharing, or something else.

### **6** Where is it going?

In addition to developing policies that address privacy in these new learning environments, some institutions are also implementing local solutions. A trend likely to continue is the practice of installing local instances of Web 2.0 applications for use by students behind an institutional firewall, where privacy can be more easily safeguarded. Similarly, learning management systems are increasingly integrating Web 2.0 applications into their tool sets, making it less necessary for faculty members to use external social networking, collaborative, or other new-media applications to meet their instructional goals. These two approaches enable institutions to maintain greater control over student records and assignments, thereby largely avoiding privacy issues. The tools themselves are evolving to allow users to implement them in a variety of ways that allow use while protecting privacy. This does not remove the need to continue to explore and adjust policies or practice, but it does provide alternatives.

### **7** What are the implications for teaching and learning?

Interest in the use of cloud-based and Web 2.0-style tools in the curriculum will only increase over time. Finding a balance between the use of these tools and protecting educational privacy is an issue that all institutions must address sooner or later. One approach is to articulate and disseminate institutional policies and recommendations in this area, so that faculty members can make informed choices about what tools to use and how to direct their students in carrying out their assignments. Providing similar training to students will enable them to become good stewards of their online presence, with an eye to its potential influence on their academic and professional lives.

**EDUCAUSE**

EDUCAUSE is a nonprofit membership association created to support those who lead, manage, and use information technology to benefit higher education. A comprehensive range of resources and activities is available to all EDUCAUSE members. The association's strategic directions include focus in four areas: Teaching and Learning; Managing the Enterprise; E-Research and E-Scholarship; and the Evolving Role of IT and Leadership. For more information, visit [educause.edu](http://educause.edu).