

Privacy can be an important issue to many individuals. For example, most people would not want their academic record posted on the Web for anyone to see. Many also would not want their class time streamed as a video online without their consent. For some, a shift to online education may even be due to a desire for anonymity and privacy. In the online era within a Web initially designed to share information, we must consider that not all information should be shared in the same way. In many circumstances, privacy can be considered an individual right that government should serve to protect. By providing guidelines in listed situations, this article will address specific issues of online privacy in an educational context and regulations that the government and other institutions have put in place to protect that privacy.

FERPA

FERPA is a U.S. federal law providing mainly for the privacy of educational documents. FERPA stands for the Family Educational Rights and Privacy Act of 1974 (FERPA, 20 U.S.C. § 1232g; 34 CFR Part 99). You might be surprised at how long it has been around, since it has received so much attention due to the growth of online education, but privacy has been an issue for as long as two people lived in sight of each other. The text of the Act is contained in Title 20 of the U.S. Code and is available in many online sites such as the Electronic Privacy Information Center <<http://www.epic.org/privacy/education/ferpa.html>>. In general, FERPA provides students with the following rights:

- To see your educational record

- To seek amendment to that record
- To consent or not consent to the disclosure of that record to others (some information may be released without student permission under certain circumstances such as court proceeding requirements)
- To file a complaint with the FERPA office in Washington, DC.

Educational record can be a deceiving term, because it can mean many things to many people. It might be easier to first consider what is **not** part of one's educational record. Private notes of the instructor on the student, medical records in any school-run medical facility, campus police records, and anything that does not pertain to the educational process of that student individually are not part of one's educational record. The educational process can take many forms though, including notes, computer files, and even verbal discussions. To an online educator, this would mean that any exchange occurring in the class in which a student is involved becomes a part of that student's educational record. Thus, not only is the exchange protected under copyright, as the student would own his/her contribution, the exchange is also protected under FERPA. Finally, FERPA designates some information as 'directory' information in higher education, allowing such things as name, addresses, and phone numbers to be divulged; however, students retain the right to require that such information not be disclosed.

FERPA rules change somewhat depending on the age of the student. For a student 18 years of age or older, unless the student is dependent on the parents or legal guardian as defined by the Internal Revenue Service, the student must sign a consent form before parents can access his/her educational record. In general, parents or legal guardians of a student under the age of 18 control the student's records, unless the student is legally independent.

PRPA

The Protection of Pupil Rights Amendment (PRPA, 20 U.S.C. § 1232h; 34 CFR Part 98) protects students under the age of 18 from unwanted participation in U.S. Department of Education funded surveys, evaluation, or other data gathering forms in which personal information may be revealed. It does not refer to the reporting of that data or its research use, rather, PRPA pertains to the actual allowance for the collection of the data in the first place. Other provisions allow for the parental inspection of materials that may be used in connection with the project as well. The purpose of the act is primarily to protect students from divulging protected information unwittingly.

For a more thorough treatment of FERPA and PRPA or for additional information, perform a Web search or visit the Family Policy Compliance Office Website

<http://www.ed.gov/policy/gen/guid/fpco/index.html>.

COPPA

Another important piece of legislation with regards to privacy that could impact online education is the Children's Online Privacy Protection Act of 1998 (COPPA, 17 U.S.C. § 1301-1308). The full text of the code is found online at the Federal Trade Commissions Web site <http://www.ftc.gov/ogc/coppa1.htm>. This act specifically protects the privacy of those under the age of 13 when online. Basically, it is unlawful for operators of an online service to collect personal information from those under 13 without meeting several provisions. These provisions include: a clear privacy notice, notice of how the information is collected and for what it is collected, nondisclosure of information to third parties must be an option, parents have the option to have the child's information removed, and verifiable parental consent. Additional restraints exist for

public disclosures of information gathered without a reliable method of consent such as a verified credit card number, postal mail consent form, or digital signature.

COPPA is aimed primarily at commercial ventures, but has applications to online education when information is collected in a survey in such a way that it might be shared or used outside of the immediate teacher-student educational context. It can also cause difficulty when using external for profit services such as plagiarism detection sites. Many such as TurnItIn.com specifically state that the service is not intended for use by students under the age of 13.

Additional information on how to comply can be found on the FTC Website.

<http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm>.

FoIA

The Freedom of Information Act (FoIA) was designed to provide necessary access to information for those with a right to obtain that information. However, the FoIA applies only to federal agencies and does not create a right of access to records held by state or local government agencies. Each state has its own public access laws that should be consulted for access to state and local records. Therefore, although sometimes cited, the U.S. FoIA is usually not of issue in online education.

Guidelines

What does all of this mean to the online educator? Above, I was attempting to bring to light the key points from several pertinent regulations concerning privacy in the online context. Below I present a list of guidelines that help explain what an instructor needs to do in order to remain compliant with these regulations. These guidelines are simplifications, and exceptions will exist. They are not intended as legal advice, but rather a set of principles that one can use to

guide further exploration of the issues. It should also be noted that interpretations of the law will change as the student turns 13 and again when the student turns 18.

1. Avoid RSS feeds for any discussions that may involve assignments or that may divulge course participant information. Why? – RSS feeds are not secure. Anyone with the correct address could ‘listen’ to your feed.
2. Avoid discussing grades in a synchronous chat room or discussion forum. Why? – First you have to question whether the person you are chatting with is actually the person identified. Has some guarantee been used to verify the person’s identity such as video imaging or IP matching with a ‘home’ machine? Secondly, someone unauthorized could be looking over the shoulder of the person if the access site is public. Discussion forums and synchronous chats are usually archived in some way as well. This archive should be deleted if it contains any discussion of grades or assignment feedback. Any such forums should be limited in access to only the instructor and the individual being discussed if used. For example, an instructor may use a private discussion forum in a secure course management system to divulge grade information.
3. Avoid returning graded assignments through email. Why? – Email may be read by someone unauthorized to view feedback. Such a person may include tech support with the person’s service provider. Email furthermore provides even more identification of the user than just the name alone, as institutional affiliation and account username are often included in email addresses.
4. Make accommodations for the use of guest lecturers. Why? – Unlike a face-to-face course, online guest lecturers often have access to discussions not related to the topic of the given lecture. S/he may also have access to a full roster of students in the given

course and their email addresses. Policies written into some registration agreement or student policy should address the allowance for guest lecturers. Guest lecturers should also be informed about the privacy of non-discussion oriented information and locked out of such information if the course management system allows.

5. Allow for anonymity or limit available information to the public and other students.

Why? – Some students, especially if under age, will have need for some level of anonymity. Some may be taking online courses specifically for this reason. While many getting-to-know-you ice-breaking activities can help to create an online community of learners, some learners may want or need an online persona separate from their real identity.

6. Address data security as a whole. Why? – If student data is in some way compromised, it is your ethical duty, and in some states legal duty, to disclose the situation to the students and possibly parents of those involved. Furthermore, you may be held partially liable if this information is used for illegal purposes if you were negligent in your security practices.

7. Address student privacy as a whole. Why? – Many regulations above require clear and easily accessible privacy information to be available to students and parents.

Furthermore, as stated for 6 above, theft of data could have consequences. Additionally, you could provide a technical support module in any online student orientation including information on such items as virus protection (which can include key stroke compilers), digital signatures, secure email, directory information suppression, etc.

8. Allow for technical support access to the course. Why? – Technical support may/will need access to your course to help students if an issue such as a problem loading a

required Java application occurs. Technical support such as this may be beyond pedagogical reasoning. If they could also have access to student accounts through administrative access, a clear policy should be available allowing for such activity without violation of the law.

9. Properly allow for plagiarism detection. Why? – For children 13 and under, you may not be able to use plagiarism detection sites. For older students, documents should always be submitted by the student and prior to any grading. In this way, the document has not yet entered into the student's record.
10. Additional provisions may be necessary for educating students under the age of 13 in an online environment. Why? – See COPPA above. That being said, additional provisions should be made for educating anyone about their rights based on FERPA, but it is especially important for children under 13 and their parents.
11. Maintain/host course management and/or quizzing systems locally when possible. Why? – Although some may see it as financially more feasible to maintain a course management system externally, there can be issues in that student data will be stored on a system that the school itself does not control with regards to security. Others may have access to roster lists for example. Any external host should be questioned about privacy requirements and legal compliance.
12. Utilize IP tracking when privacy provisions allow for it and the need is appropriate. Why? – IP tracking involves several issues. First, there are the ethical questions of tracking of student access, but at the same time, tracking of IP access to a site allows for determining unusual access to the site, which may send a red flag that someone is trying to illegally access information. Tracking can also be used on the detection of cheating,

for example when a student account is always accessed from a different IP address when tests are taken.

13. Provide a support number to quickly address any issues that may arise. Why? –

Provisions in several areas of the law require that easy contact be available when students or parents have questions about privacy and its protection. Easy access to support also allows the institution to make a quick change if a problem is discovered.

14. Survey data from students that is used for outside the classroom research generally needs

consent and especially needs parental consent when students are under the age of 18.

Review by an institutional authority is usually also required if the institution accepts government funds. Why? – Informed consent becomes more of an issue with younger students, but still applies to all ages. The reason it applies to this discussion is that a lack of personal identification in any survey is always a plus, but is not always enough to insure acceptance under the law.