4-1-2009

The Ginsburg Group: Technology: How to Stay out of Court

Jennifer Ballard
Western Kentucky University, Jennifer.Ballard@wku.edu

Lee Maglinger
lee.maglinger@ky.gov

Alisha Orosz
Western Kentucky University, alisha.orosz@wku.edu

Mandy Skinner
Western Kentucky University, mandy.skinner@wku.edu

Kevin Thomas
Western Kentucky University, kevin.thomas@wku.edu

The Ginsburg Group

Technology: How to Stay Out of Court

Jennifer Ballard
Lee Maglinger
Alisha Orosz
Mandy Skinner
Kevin Thomas

Technology: How to Stay Out of Court

Opening Thoughts by the Ginsburg Group

For professionals in higher education, it is our responsibility to stay on top of the ever changing landscape of technology at our colleges and universities. In order to provide the best and most convenient services, it is our objective to continue to expand the walls of higher education into the global boundaries of technology. For the purpose of this paper, the Ginsburg Group has focused on five different areas regarding the use of technology. In these areas, the information provided is our thoughts and best advice in how institutions of higher learning can avoid the courtroom.

The following pages will dive into information on a wide variety of topics that the Ginsburg Group felt was important in discussing "How to Stay Out of Court." Each chapter presented will contain information regarding the topic and then will finish with reference for that chapter. The five chapters we broke the information down to are:

- Chapter One: FERPA
- Chapter Two: Electronic Communication
- Chapter Three: Plagiarism
- Chapter Four: Electronic Content
- Chapter Five: Outsourced Technology

As a group, it is important to note that we are students in a Counseling and Student Affairs course who are putting our best attempt forward in regards to the law. The information we are providing in the pages to follow are the culmination of a semester of information received in our Counseling and Student Affairs course that is titled "Parameters of Law/Student Affairs." When it comes down the specifics of each area, it is always smart to consult your university attorney.

Thanks for taking time to read our information on "How to Stay Out of Court."

Sincerely,

The Ginsburg Group

Jennifer Ballard, Lee Maglinger, Alisha Orosz, Mandy Skinner, Kevin Thomas

Chapter One: Ways to Avoid Court: FERPA

According to the US Department of Education, the Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of a student's educational records. This law applies to all schools that receive funds under an applicable program of the US Department of Education. FERPA provides protection of educational records for students who are either eighteen OR attend a school beyond the high school level (US Department of Education, 2008). Another important thing to remember is that FERPA does not just protect the rights of current university students. Educational record information regarding former students cannot be released as well without permission from the student. This information will be the basis for a number of legal courses at the higher education level. The purpose of this chapter is to inform you of steps to take when trying to avoid going to court with regards to FERPA (University of Rhode Island).

It is important to note that FERPA came into law before technology became what it is today. FERPA became law in August of 1974. That being said, many universities did not have the elaborate networks and systems we do have today (Lowe, 2005). Furthermore, thirty-five years ago the majority of all people had never heard of email, text messaging, or other words regarding the technological boom we have experienced as a culture over the last fifteen-twenty years. This means that the courts must interpret much of the legal cases involving FERPA. Below is listed "Five Tips on How to Stay Out of Court Regarding FERPA and Technology."

Five Tips on How to Stay Out of Court Regarding FERPA and Technology

1. **Train Your Employees.**

How is it possible for any employee to understand the law if they are never trained or taught the information? Most universities have in-depth online training for all new faculty and staff members. More than that, it is important to build FERPA training for the hiring of each student staff, part-time staff, and all faculty members.

Sylvia Kelley of the Dallas Business Journal states, "You have to train people for the right reasons. Certainly, improved business performance is very important. Good training will yield higher profits, reduced costs, employee retention, improved production and many more tangible, positive results. We should also remember what sometimes seem to be the less tangible reasons for giving people valuable training opportunities. When we invest in our employees by providing training, they feel better about themselves, they want to make a quality contribution, they often deal with personal situations in a more positive manner and they can mentor and help others. We all benefit" (1999).

For examples of training sites, please visit any of the following FERPA training sites:

- ✓ University of Arizona Web Course on FERPA (http://www.registrar.arizona.edu/ferpacourse/)
- ✓ University of Illinois Tutorial (http://registrar.illinois.edu/staff/ferpa_tutorial/index.html)
- ✓ University of Texas of the Permian Basin (http://aa.utpb.edu/registrar/ferpa-training-module/)

2. **Make Your Policies Known.**

As stated in an article by Scott Lowe of TechRepulic, "schools that record information about student's network use, including Web sites visited, contents of e-mail messages, and more, may be required to protect that information as stringently as other person information, assuming that the information in question could personally identify a particular student." If the information is stored on institutional servers, this information could be considered part of a student's educational record (2005). This goes back to the training aspect for faculty and staff. If they are aware of this type of action by the university they can better inform students of the network use policies on their campus. For information technology departments, it is also creating an awareness of what is being monitored on university servers. Students should be aware of this type of action.

3. **People Should Only Have Access If They Need Access.**

FERPA requires faculty and staff to adhere to strict policies regarding a student's educational record. This requires that only the appropriate people have access to sensitive information. Offices such as Information

Technology need to closely monitor account permissions (Lowe, 2005). One of the best examples of this is in what the IT Department at Western Kentucky University does with its online systems.

Each office that hires a new employee or would like access to the online systems must go through a specific training that focuses on correct use and information on how to use systems such as Banner and TopNet. If departments would like to request other people to have use of these systems, specific regulations are placed on those accounts. In the Academic Advising and Retention Center, student staff members called Peer Advisors, have access to student's schedules for use when meeting with students in academic struggles. Unlike many administrators on-campus, however, they do not have access to personal information or many of the other tabs that provide sensitive information about the student.

4. Access of Educational Records.

As stated in FERPA 101 from the University of Rhode Island, "a school official should only access student's education record if a legitimate educational interest exists with respect to that student and that record" (University of Rhode Island). What does this mean? For university officials, it means having a legitimate reason to view a student's educational record.

Based off a personal example, in a training done through the Academic Advising and Retention Center, Western Kentucky University Registrar, Frieda Eggleton, is asked to come in and speak each semester regarding FERPA. One of the items she provides is a quiz for FERPA policy. In this quiz a faculty member said they will get onto TopNet before the semester starts and see how their students did in previous semesters to gage how this next semester will go for this person as a faculty member. This is just one example of a lack of "legitimate educational interest" as described in FERPA. Just because a person can view educational records of students, it does not mean they have the legal or "legitimate" right to view the information.

More and more schools now have the capability to store notes, messages, or other electronic communication in online databases. It is important that university officials do not put personal notes in a student's file as they will become accessible to the student. A great example of this is in the AdvisorTrac system used at

campuses' across the country (and at Western Kentucky University). In this system you are able to make notes regarding the advising appointment for your advisees. What is important to remember is that these notes are a student's educational record. As a campus, advisors are informed to make personal notes separate from the AdvisorTrac system. For example, if an advisor meets with a student who they feel need to go to Counseling and Testing, it is okay to list that in a student's file as a referral to that office but the advisor should not include in the notes that the advisee seemed completely out of their mind. How you enter the information and what you enter is important because it is part of a student's educational file.

5. Information Sent Through Email, Phone Calls, Social Networking Sites, Etc.

University officials must also be aware of how they communicate with students regarding their educational record. As a whole, if it is possible to have face-to-face communication with a student that should always be the preferred method. There are several reasons why this is a positive practice to use when trying to stay out of court (University of Miami-Ohio).

A. You never know who has access to a student's email account. If you are going to use email to communicate with a student, it is a helpful tip to always use the student's university account. For example, at Western Kentucky University students all have a university assigned email address. Typically, in the TopNet system they also have a "preferred email" address listed or "alternate email" address listed. Those emails are not official emails of the university and should not be used to communicate regarding specific academic information such as grades (University of Miami-Ohio).
B. Phone calls are effective and often direct way of communicating with a student. When it comes to information such as grades, it is good practice to avoid communicating that information over the phone. How is it possible for university officials to know who they are speaking to on the phone? It is not possible, so it is a safe practice to avoid giving away that information (University of Miami-Ohio).
C. Social networking sites have also become a way to communicate with students on college campuses. Again, it is important that universities require that information, such as grades, be given in the

appropriate manner. Social networking sites are not that appropriate source. Even more than the third party vendors that will be discussed later, most social networking sites do not have a contract of responsibility to the university. This means, in many cases, those social networking sites have control of the content. An example of this type of situation occurred recently with the social network site, Facebook.com."

Their policy regarding content states, "You hereby grant Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, translate, excerpt, adapt, create derivative works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof subject only to your privacy settings or (ii) enable a user to Post, including by offering a Share Link on your website and (b) to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof. You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content" (Waters, 2009).

References

(2008, 12). U.S. Department of Education. Retrieved April 1, 2009, from Family Educational Rights and Privacy Act (FERPA) Web site: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

Kelley, Sylvia (1999, 10). Dallas Business Journal. Retrieved April 2, 2009, from Weighing the importance of training for employees Web site: http://www.bizjournals.com/dallas/stories/1999/11/01/smallb3.html.

Lowe, Scott (2005, 07). TechRepublic. Retrieved April 14, 2009, from 10 things you should know about the Family Educational Rights and Privacy Act (FERPA) Web site: http://techrepublic.com.com/i/tr/downloads/home/10_things_you_should_know_about_ferpa.pdf.

The University of Texas of the Permian Basin. Retrieved April 27,2009, from FERPA Training Module Web site: http://aa.utpb.edu/registrar/ferpa-training-module/.

University of Arizona. Retrieved April 24, 2009, from Family Educational Rights and Privacy Act of 1974 (FERPA) Web Course Web site: http://www.registrar.arizona.edu/ferpacourse/.

University of Illinois. Retrieved April 22, 2009, from FERPA Training Web site: http://registrar.illinois.edu/staff/ferpa_tutorial/index.html.

University of Miami (Ohio). Retrieved April 21, 2009, from FERPA Tips for Faculty & Staff Web site: http://www.units.muohio.edu/generalcounsel/Documents/FERPA%20for%20Faculty%20and%20Staff.pdf.

University of Rhode Island. Retrieved April 14, 2009, from Introduction to FERPA: Family Educational Rights and Privacy Act Or FERPA 101 Web site: http://www.uri.edu/es/forms/pdf/faculty/ferpa.pdf.

Walters, Chris (2009, 02). The Consumerist . Retrieved April 22, 2009, from Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever." Web site: http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.

Chapter Two: Ways to Avoid Court: Electronic Communication

It is becoming more evident that employees, staff and faculty are using email on a daily basis at work. According to the New Hampshire Business Review, "80% of companies use email" (Moore, 1999, p. 27). Another report states that as much as 90% of all documents and correspondence are created and maintained in electronic formats" (Seaver, 2007, p. 1).

As a result, this dependency and reliance on technology has created a new set of stressors for both employee and employer. It has also caused a new set of issues with respect to employee privacy. In the past employee privacy was something taken for granted. With the advent of email and the ability to monitor it, that may be a thing of the past.

"The trend of companies monitoring employees' email and phone usage is continuing according to the results of the most recent annual Electronic Monitoring and Surveillance Survey conducted by the American Management Association (AMA) and the ePolicy Institute" (Nancheria, 2008, p.12). In this report it also noted that one-quarter of employers have fired employees for breaking company policy concerning email or internet use. Terminations for email miss use were 64% for breaking company policy, 62% for use of offensive or inappropriate language, and 22% for breaking confidentiality.

Employers are monitoring employee's computers to a greater degree than in the past. "Most US based companies assume that employees have a constitutional right to privacy. However, constitutional rights to privacy are generally inferred through the US Constitution's 4th Amendments rights to freedom from unreasonable search and seizure. Furthermore, these specific freedoms usually apply only to state actions" (Nord, McCubbins, & Nord, 2006, p.2).

The Electronic Communication Privacy Act (ECPA) is the primary legislation dealing with employee privacy. However, "there are three exceptions under the ECPA that effectively eliminates any expectation of privacy an employee might have to his or her employer" (Nord, et. all., 2006, p.3).

These three exceptions are A) "provider exception", where the employer is providing the email service, then the employer is protected from employee privacy; B) "ordinary course of business", that provides a definition of an electronic device which excludes the employer from the ECPA; and C) "consent exception", that states if at least one party to the email gives consent to interception or is the party who intercepts the communication, then the ECPA has not been broken.

"In *Smyth v. The Pillsbury Company,* Smyth sent his supervisor emails that contained inappropriate and unprofessional comments from his home computer. The supervisor received the emails over the Pillsbury's email system. At a later date the company intercepted those emails and terminated Smyth's employment" (Nord, et. all., 2007, p.3).

"A senior professor asked permission to post an announcement promoting an antiwar rally on a college's official email announcement list. Although the rally was to take place on the campus, it was not a university-sponsored event. His supervisor explained that it would be inappropriate, and unethical to use the college's official communication medium to announce events unrelated to the conduct of official college business" (Olson, 2007, p.1). The professor was shocked at this response and replied that "surely, everyone in the college is against the war." The supervisor responded that university's resources were not to be used for personal business.

In a similar case, "A department chairman was reprimanded for using his office computer and email account to engage in day trading on the stock market. He closely monitored stock fluctuations throughout the day, constantly buying and selling shares. He even bragged to colleagues that he was raking in the dough" (Olson, 2007, p.1). The department chairman was very shocked that his behavior was against the university's email policy when it was scrutinized by auditors and judged as misusing state property and conducting private matters during working hours. He was lucky to have gotten off with a reprimand.

Many employees and staff at a university see email accounts as a fringe benefit provided with no strings attached. The plain fact is that computers are assigned by the university, and as such by the state, as a tool to increase the efficiency and effectiveness of the work. That is why they have the sticker with the number that states

"Property of the Commonwealth of Kentucky" on it. The same as an office copy machine. Yet how many employees make personal copies on those machines. The same then can be said about the use of email and internet.

Most universities do not frown on the use of email to invite a colleague or friend to lunch or dinner, but they do so when the use of email becomes extensive, e.g. selling or buying items on eBay, or political advocacy issues. The example above of buying or selling on a day trade is an activity that clearly breaks most university policy concerning email usage. "It is the equivalent of petty theft at the supermarket, where each person has their own personal threshold as to what is morally acceptable. Some think nothing of popping a few grapes into their mouths while in the produce section, while others justify keeping an extra $20 bill that the cashier mistakenly gave in making change" (Olson, 2007, p. 2). No matter where you draw the line it is still theft.

How then can an employee of the university make sure that he/she is using the email system correctly? One way is to establish external email accounts for personal use. These would make "clear boundaries between university business and personal or recreational use. Maintaining a personal account would not only help avoid the ethical transgressions, it could also protect you from unexpected legal trouble. A common legal tactic used is to obtain someone's email messages through a public-information request" (Olson, 2007, p. 2). Universities require a certain amount of archive of email because they own them. They were produced by an employee, using state equipment on a university email account at their work space also provided by the university.

A second and probably more secure way to insure is to have a clear university electronic communications policy and a yearly training on the ethics of email usage. A California Appellant Court ruled that at a minimum this type of policy should contain statements, signed and read by the employee, to the effect that:

1. Electronic communication facilities provided by the company are owned by the company and should be solely used for company business.

2. The company will monitor all employee email usage. It should state who will review the information, the purposes for which the information may be used, and that the information may be stored on a separate computer.
3. The company should keep copies of the email passwords.
4. That the existence of a separate password is not an assurance of the confidentiality of the communication or other "protected" material.
5. The sending of any discriminatory, offensive, or unprofessional message is strictly prohibited.
6. The accessing of any Internet site that contains offensive or discriminatory content.
7. The posting of personal opinions on the Internet using the company's access is strictly prohibited.
8. Clearly stated repercussions to violators of company policy" (Nord, et. All., p. 5).

The second part of this chapter is concerned with the use of email by students through the university's email system. The case that is presented here is *Murakowski v. University of Delaware.* In this case a 19 year old sophomore at the University of Delaware began using the university's email system to post compositions that were crude, immature and highly offensive. The university had a policy that allowed students to use its system provided they abide by the Policy for Responsible Computing. The university took Murakowski through their disciplinary process and won the case all the way up to and through the Appellate Board. "In denying Murakowski's appeal, the Appellate Board found that he had not presented sufficient grounds, and no changes were made to the original punishment. In this case, the Board also concluded that the sanctions were not only appropriate, but not harsh enough" (Pavela, 2008, p. 18).

What then should be done to help with the problems associated with student use of email at a university? Again, students should be held to the same policy that employees are. In addition, both employees and students should be involved in ongoing training about the ethics of use of emails. "Illinois mandates that all state

employees, including faculty and staff members, and students at all public universities take an online ethics course" (Olson, 2008, p. 2).

Email use provides its users with many conveniences and efficiencies like no other tool to date. The problems it produces will continue to present questions for some time to come. The battle between email monitoring and workplace privacy is only beginning. State and federal litigation has only begun as we work to strike a balance between organization concerns over non work related activities and employees workplace privacy.

References

Moore, J., 1999. *New Hampshire Business Review,* October issue #23 as retrieved April 22, 2009, from ERIC database.

Nancheria, A., 2008. *American Society for Training & Development,* as retrieved from http: anancherla@astd.org on April 22, 2009.

Nord, G., McCubbins, T., & Nord, J. 2006. *Association for Computing Machinery.* E-Monitoring in the Workplace. Oct. vol. 23.

Olson, G. 2007. *Chronicle of Higher Education.* The ethics of technology, as retrieved February, 2009 from ERIC database.

The Pavela Report: Law & Policy in Higher Education, 2008. Retrieved from http://docs.google.com/view?docid=dfdpvzp9_1242hfjktjht on February 2, 2009.

Seaver, G., 2007. *Chronicle of Higher Education.* The new legal advice: don't press the delete button, as retrieved February, 2009 from ERIC database.

Chapter Three: Ways to Avoid Court: Plagiarism

Most colleges and universities have seen a rising trend in plagiarism. Sixty-six percent of sixteen-thousand students from thirty-one prestigious U.S. universities have cheated at least once. Twelve percent of those reported that they were regular cheaters. That means that nearly seven out of ten students cheat, and that at least one of those ten students cheats all the time (Overbeck 2000). The University of California-Berkley estimated that between the years 1993-1997 plagiarism rose seven hundred and forty-four percent (Overbeck 2000). Plagiarism has always been a wide spread problem, but now with the use of the World Wide Web, it has become even more of a problem for universities. This section of the technology handbook will give student affairs professionals background information on plagiarism (laws, statues, and court cases), a clear definition of plagiarism, how plagiarism often happens, and steps to prevent plagiarism.

Section 3.1: Plagiarism – Laws, Statues, and Court Cases

Before we dig in to the definition of plagiarism and other words often associated with plagiarism, let's look at some background information about plagiarism.

Copyright laws: Copyright laws make it illegal to reproduce someone else's expression of ideas or information without permission.

Before 1989 items were only copyrighted if they included the copyright symbol (©). However in 1989 the US started to adhere to the Berne Convention for the Protection of Literary and Artistic Works. The allowed works to be copyrighted with or without the copyright symbol (US Copyright Office 2009). Students who don't fully understand that works can be copyrighted with or without the copyright symbol are more likely to unintentionally plagiarize. So it's very important that as a professor you make sure and stress the point that unless works are a part of the public domain (which is address later in this section) they must cite every source they use or they will be guilty of plagiarizing.

Trademark law: Protects symbols or other artistic work that an individual has created, so that their work cannot be plagiarized.

This law is different from copyright law because unlike copyright law, which allows for criminal penalties and civil damages, trademark law is perused entirely though private lawsuits. So in order to stop someone from committing trademark infringement the individual has to file suite with either a state or federal court to stop the infringement.

Court Cases Dealing with Plagiarism:

Most plagiarism cases are settled outside of court or charges are dropped before going to court. However the ramifications are still the same. Once you have been accused of plagiarism you always have the reputation of being a plagiarizer, whether you actually committed the crime or not. The president (Meehan) of Jacksonville State University (JSU) in Alabama is being accused of plagiarizing his doctoral dissertation at the University of Alabama. It is being alleged that Meehan took significant portions of Boeings' dissertation and used it in his dissertation. Boeing is not stating if he thinks that Meehan plagiarized his works but faculty members of JSU are claiming that he plagiarized. More details will be forthcoming as the investigation progresses (Associated Press 2009).

Schools can sometimes use plagiarism to hide a true reason for the dismissing of a faculty member, as was the case for a tenured faculty member at the University of Colorado. Ward Churchill wrote a disturbing essay days after 9/11 in which he referenced some of the World Trade Center victims "little Eichmann's". This obviously upset people at the university and was essentially the reason (according to Churchill) he was fired. The university claims that Churchill was fired because he repeatedly fabricated his research, plagiarized others' work and strayed from the "bedrock principles of scholarship" (Denver News 2009).

Churchill sued the university claiming that he was falsely fired. A jury found that the University of Colorado had wrongfully dismissed Churchill. They found that Mr. Churchill's political views had been a

"substantial or motivating" factor in his dismissal. He was awarded $1 in damages and a decision has not been reached as to if he will be reinstated or not (New York Times 2009).

The two legal situations that are listed above are just two of the many legal disputes that can arise when people are accused of plagiarism. In the next section we'll deal with what plagiarism is and how it happens.

Section 3.2: Plagiarism - What Is It and How Does It Happen?

There are many definitions for plagiarism. The most accurate and the most detailed description of plagiarism are found in the Merriam-Webster Dictionary.

Plagiarism: 1) To steal and pass off (the ideas or words of another) as one's own, 2) To use (another's production) without crediting the source, 3) To commit literary theft, 4) To present as new and original an idea or product derived from an existing source.

The definition is very clear about what is defined as plagiarism, anything that is not your own that you pass off as your own. To better help your students understand the seriousness of plagiarism you can relate plagiarism to identify theft. In today's society everyone should be well aware of what identity theft is (identity theft is when someone takes your identity and says it's theirs). Just as there are serious repercussions for stealing someone's identity there are serious repercussion for plagiarism.

There are several other definitions associated with plagiarism that you also have to know and understand before you can fully know what plagiarism is and how to prevent it. The following definitions will help you to better understand what plagiarism is and how each can impact plagiarism.

Citation: The act of directly quoting or giving intellectual credit to another (University of Alberta Libraries 2009). Students and faculty often cite references improperly. Most of the time (although there are some exceptions) students/faculty don't intend to plagiarize. By actively teaching/reminding your students how to properly cite references your university will stay out of court and hopefully see a down turn in the number of plagiarism cases its judicial board reviews. As a faculty member by constantly teaching your students how to properly cite

references you'll be taking steps to safeguard yourself from improperly citing references, which will help you stay out of court and protect your educational integrity and reputation.

Cyber-Plagiarism: Copying or downloading in part, or in their entirety, articles or research papers found on the Internet or copying ideas found on the Web and not giving proper attribution (University of Alberta Libraries 2009).

Cyber-Plagiarism is a subcategory of plagiarism. Students have better access to the World Wide Web which is making cyber-plagiarism more common. Often students don't have the required skills they need to properly research items for their own research papers. They often think that if they found their information for their papers on the internet that they don't have to give credit, they associate information on the internet as public domain (which is discussed later in this section). There are new programs and software systems that are making identifying cyber-plagiarism easier. By informing your students that you aware of and will be checking for cyber-plagiarism you will be taking proactive steps to help your students stay out of court and out of judicial board reviews. As a faculty member you should be aware of the consequences of cyber plagiarism. As you do research for your research projects, you should be acutely aware of how you cite internet sources so that you are not accused of cyber plagiarism, which will keep you and the university happy.

Deliberate Plagiarism: the action of copying another's paper with the intention of representing it as one's own (University of Alberta Libraries 2009).

Deliberate plagiarism should be addressed to your students. You should state your schools policy on plagiarism and inform students what could happen to them if they are caught plagiarizing. As a faculty member you should know to avoid deliberate plagiarism at all cost. Always properly cite your sources and always ask someone if you're not sure on how to cite something or if something should be cited or not. If you are found to be deliberately plagiarizing you could possibly lose your job and ruin your educational reputation.

Public Domain: Material that may be reproduced, communicated, or preformed without credit being given (University of Alberta Libraries 2009).

Students sometimes misunderstand what is considered public domain, and as a result plagiarism results. As a faculty member you should inform your students what is considered to be public domain and what is not public domain, by doing this you'll be able to help your students better understand what is considered plagiarism and how not to plagiarize. As a faculty member by reminding your students of what is considered public domain you're also refreshing your memory as well so that you're able to keep your job and stay out of court.

Unintentional Plagiarism: Is described as "careless paraphrasing and citing of source material such as improper or misleading credit is given" (University of Alberta Libraries 2009).

If you are reminding your students about the definitions of plagiarism, public domain, citations, and cyber plagiarism, you should have no problems with unintentional plagiarism. However unintentional plagiarism happens, and usually is a result of different professors wanting different referencing styles such as APA or MLA. I would recommend that all the professors in your area require the same style so that you're students know what style is expected of them across the board. This will greatly help your students and cut down on the amount of plagiarism judicial review boards that your university sees. As a faculty member unintentional plagiarism should not happen, however you're only human and mistakes do happen. You should always be very conscientious of how you cite your references, in your paper and on your reference sheet. You should always be aware of what style you are using and follow the appropriate guidelines. Plagiarism can be detected and avoided; all it takes is a little extra time, attention, and work.

Section 3.3: Plagiarism – How to Prevent It.

Explain what "Plagiarism" means: Explain to your students what plagiarism is, even though they should already know, it never hurts to repeat yourself on this issue. Handouts with clear definitions could be utilized in order to give students a visual aid to help them in their process of finding and citing sources (iParadigms 2009)

Explain why plagiarism is wrong: Explain to your students that plagiarism is a form of fraud. Earlier in this section plagiarism was related to identity theft. Help your students understand the seriousness of plagiarism, so that they can properly equip themselves to not plagiarize.

Make the consequences clear: Let the student know that there are academic punishments, and legal punishments for plagiarism. Inform your students of the schools policy on plagiarism. Spell out what will happen if they are caught plagiarizing. Most students don't realize how serious plagiarism is until they are caught. Let them know that in some cases they can be fined anywhere from $100.00 - $50,000.00 and even up to one year in jail. Under certain state and federal laws plagiarism can be considered a felony earning the person can face a fine up to $250,000.00 or up to 10 years in jail.

Have students annotate their bibliography: Have students summarize the content and usefulness of the sources that they used. Emphasize that annotation has to be in the students own words and should specifically discuss the relevance of the source to their paper (iParadigms 2009)

Require recent and printed sources: Most online paper mills are not kept up to date. By requiring at least one current source you will be able to ensure that your students are not buying or downloading from the online paper mill sties.

Encourage caution: Encourage students to be as precise as they can. Students often plagiarize when trying to pad their papers trying to meet a page requirement.

In closing I'll leave you with a few closing thoughts. Plagiarism is an ongoing problem; it is something that is continually evolving and ever changing. As a student affairs professional plagiarism should always be a major concern of yours, because you deal with students on a daily basis and as a professional you're expected to be published and to present findings. Being constantly aware of where you get your information and how you report it. As a student affair professional you have your reputation and integrity to be aware of. If you lose one you often times lose the other, and many times you can never get them back.

References

Denver News. (2006, June 26). CU To Fire Ward Churchill. Denver News. Website: http://www.thedenverchannel.com/news/9424240/detail.html.

iParadigms. (2009). What is Plagiarism?. Retrieved April 21, 2009, from Plagiarism.org. Website: http://www.plagiarism.org/learning_center/what_is_plagiarism.html.

Johnson K. and Seelye K. Q. (2009, April 3). Jury Says Professor Was Wrongly Fired. New York Times.

Overbeck B.K. (2000). *Did You Know???*. Retrieved April 21, 2009, from Plagiarism Statistics. Website: http://iml.jou.ufl.edu/projects/Spring2000/Overbeck/stats.html.

Reeves J. (2009, April 22). Aka, college president accused of plagiarism. Associated Press, Retrieved April 27, 2009. Website: http://www.google.com/hostednews/ap/article/ALegM5jigNGLtg9PtFNelXVdVdNFVfb48wD97NP9480.

Terminology. (2009). Retrieved April 24, 2009, from University of Alberta Libraries. Website: http://www.library.ualberta.ca/guides/plagiarism/teminology/indes.cfm.

U.S. Copyright Office. Retrieved April 27, 2009, from Copyright Information Circular. Website: http://www.copyright.gov/circs/circ1a.html.

United States trademark law. (n.d). Retrieved April 27, 2009, from Wikipedia: http://en.widipedia.org/wiki/U.S._Trademark_Law.

Why Students Plagiarize. (2009). Retrieved April 22, 2009, from University of Alberta Libraries. Website: http://www.library.ualberta.ca/guides/plagiarism/why/index.cfm.

Chapter Four: Ways to Avoid Court: Electronic Content

In 1998 the Digital Millennium Copyright Act (DMCA) was implemented in order to account for copyright violations in the new age of digital information. "DMCA criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works and it also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself" (www.wikipedia.com). This would become the foundation of both partnerships and battles between the entertainment industry and higher education.

Although the Recording Industry Association of America (RIAA) has not discriminated towards its targets, it has largely focused on college and university students, residential students in particular. "According to the Pew Internet & American Life Project, college students were more than twice as likely as all Internet users to have downloaded music from the Internet" (Lane & Healy, p.535). The litigation campaign began in fall 2003 with 261 music fans being sued for sharing files on peer-to-peer (P2P) file sharing networks. In 2008 that number had risen to at least 30,000 lawsuits which had been filed, settled or negotiated through pre-litigation techniques. (Electronic Frontier Foundation, p.1).

The DMCA contains provisions which would allow legal protection for higher education institutions based on their cooperation and compliance; two of those specifically apply to educational institutions and are relevant to file sharing. "The Transitory Digital Network Communications, where an institution acts as a conduit of network traffic. Residence halls generally fall into this category because the institution provides the network connectivity but does not own the end-user equipment. The second is defined as Information Residing Systems, where systems owned by the institution are involved" (Wada, p. 19). Under this policy educational institutions were at minimum required to adopt and implement a policy of terminating user accounts upon repeated offenses. They were required to determine a Designated Agent who would be responsible for receiving, processing and responding to copyright infringement notices and the institution could not have prior knowledge of infringements.

Ten years after the original DMCA was passed the bar was raised for educational institutions through the Higher Education Opportunity Act (HEOA) which was signed into law in 2008. The U.S. Department of Education is currently trying to translate these regulations into acceptable practice, but the HEOA continues to provide protection for universities in compliance yet it created a more specific set of expectations and standards to abide by. "The law requires colleges to inform students of institutional and criminal penalties for unauthorized file sharing, to effectively combat copyright violations with a variety of technology-based deterrents and to offer alternatives to illegal downloading" (Lipka, p.1). The controversial wording of these requirements is compounded by the potential penalties for non-compliance such as resulting in the loss of federal funding. Most institutions already have policies and programs in place to educate students, but the additional requirement to provide alternatives is currently being highly debated. The U.S. Department of Education expects the rule-making discussion and process to continue throughout 2009 with regulations most likely going into effect July 2010. (Wada, p. 20).

However, in the meantime there are many examples of good practice from various educational institutions and suggested guidelines which provide protection for universities in a short-term capacity while educating students and working to rectify the problem in a long-term capacity. This system of alternatives can be especially important to higher education because of the high cost associated with processing claims and regulating student behaviors. "A recent study found that, per institution, between $350,000 and $500,000 a year is spent tackling the piracy problem. IT personnel alone spend a mean time of 750 hours at public institutions dealing with allegations of infringement" (Jones, p.1).

Educause, a non-profit association whose mission is to advance higher education by promoting the intelligent use of information technology, suggests that universities focus on the following five areas to respond, correct and educate students on their campus. These are strictly broad guidelines which will help to satisfy the HEOA requirements but also to cultivate a sense of responsibility and understanding in students when it refers to intellectual property, including music file-sharing.

- Institutional Policies
    - Create a statement which specifically outlines the legal and financial implications of copyright violations as they pertain to the university. This should detail what is considered unacceptable behavior on academic networks in classrooms, campus and in residence halls. The policy should be made available through brochures, flyers, the code of student conduct, and terms and conditions of enrollment.
- Student Awareness
    - Create a consistent and on-going campaign to develop student awareness about the institutional policy, copyright law, and the overall significance of finding legal alternatives to music downloading. This process should be largely educational and target students from a variety of venues and informational avenues.
- Student Judicial Process
    - Many universities have already implemented judicial processes which either coincide or compliment technological policies. In example, several of the following techniques are currently employed on campuses across the country: disabling connectivity for a particular period of time, potential reconnectivity fines, completing educational tools such as quizzes, essays and partaking in applicable video viewings, mandatory discussion groups and individual meetings with Chief Judicial Officers as well as Dean of Students. "Implicit in any judicial response is the teachable moment: holding students accountable for their actions but giving them an opportunity, at each step, to change their behavior."
- Legal Options for Digital Entertainment
    - The HEOA does not specifically state what alternatives are expected and/or acceptable but the market for legal alternatives is growing and changing daily. The following are just a few of the currently available options: iTunes, Amazon, Rhapsody, Amarok, Archive.org, Jamendo, Magnatune, and MusicBrainz. Most recently the attention has been focused on "blanket licensing" which is also

referred to as voluntary collective licensing. (von Lohmann, p.1). According to the Electronic Frontier Foundation, Warner Music began the discussions with various universities but EMI as well as Sony-BG are openly considering the idea. This particular project is entitled Choruss and "universities would pay a standard fee in exchange for an end to the John Doe subpoenas seeking student identities, DMCA notices, lawsuits against students, and legislation mandating copyright surveillance of campus networks. Students would then pay to be able to download whatever they like, using whatever software they like, in whatever format they like" (vol Lohmann, p.1). Currently the RIAA lawsuit campaign has not distributed any of the collected money to the creative artists in which they are suing for, but this system would change that. All money would be divided between the artists and rights holders based on their shared popularity.

- Technology
    - The HEOA does specifically state that educational institutions are responsible for developing plans to combat the unauthorized distribution of copyrighted materials through a variety of technology based deterrents. This can be done through a variety of means including auditing network systems for files of three to five megabytes in size that are stored in musical formats such as .mp3, .wma, and .wav. Another somewhat controversial method is the use of programs which ban unauthorized software installations on academic networks. The University of Florida has pioneered a system developed by Red Lambda entitled cGrid which is being increasingly implemented across other campuses however it is has been criticized for limiting academic freedom and legal file-sharing. A more popular program which monitors P2P traffic but individually blocks unlicensed traffic is Audible Magic's "Copysense" application. Bandwidth shaping, firewall blockage and monitoring traffic levels are also ways to monitor, yet no infringe, on Internet traffic taking place on academic network.

References

Digital Millennium Copyright Act. (n.d.). In Wikipedia.com. Retrieved February 12, 2009, from http://www.wikipedia.com.

Jones, B (2008). Tackling College Piracy: At What Cost? Retrieved February 12, 2009, from http://torrentfreak.com.

Lane, J. & Healy, M. (2005). File Shar9ng, Napster, and Institutional Responses: Educative, Developmental, or Responsive Policy? NASPA Journal, 42(4). Retrieved February 12, 2009 from EBSCO.

Lipka, S. (2009). New Rules Will Push Colleges to Rethink Tactics Against Student Pirates. *The Chronicle of Higher Education*, Retrieved February 12, 2009, from http://www.chronicle.com.

RIAA v. The People: Five Years Later. (2008). Electronic Frontier Foundation. Retrieved March 2, 2009, from http://www.eff.org

Von Lohmann, F. (2008). Labels Open to Collective Licensing on Campus. Retrieved February 24, 2009, from http://www.eff.org.

Wada, K. (2008). Illegal File Sharing 101. *Educause Quarterly*, Retrieved February 24, 2009, from EBSCO.

Chapter Five: Ways to Avoid Court: Outsourced Technology

In the age of technology students are arriving on college campuses expecting 24/7 access to their records, class resources, and other university data. Students are operating on increasingly busy schedules demanding assistance beyond the typical 9-5 work day. In order to meet the increasing demands of students many universities are turning to outsourcing student data systems. The use of these systems not only satisfies student demand for easier/quicker access but it is often times more cost efficient than developing and maintaining the program in-house. When considering outsourcing there are important issues to consider, especially in relation to the privacy and security of student records.

FERPA

As previously mentioned in Chapter 1, FERPA establishes rules and regulations in relation to the privacy of students' records. As the demand for technology increased so did the need for outsourcing; however, not until recently has FERPA clearly stated how its rules and regulations relate to the outside parties (those operating the outsourced service) and the liability of the university requesting the service. In 2008 the Federal Register issued an updated version of Rules and Regulations which specifically addressed outsourcing concerns.

Outside Parties Who Qualify as School Officials

According to the report, the "broad definition of education records includes records that are maintained by a 'person acting for' an educational agency or institution (p.74814). This then supports that outside contractors do qualify as school officials as they are working as an agent for the institution. It does however clarify that the outside party "must perform an institutional service of function for which the agency of institution would otherwise use employees." This means that outside contractors can only have access to student records if they are "acting for" the university such as maintaining an online educational tool like Blackboard. Therefore, access to student records is not permissible under this clause to allow contractors to access the information to sell a product. For example, "a school may not... disclose personally identifiable information from a student's education record, such

as the student's SSN or student ID number without consent, to an insurance company that wishes to offer students a discount on auto insurance"(p. 74814).

One way to determine whether or not an outside party should have access to student records is to determine whether it serves a "legitimate educational interest." If their role serves this interest and in order to perform such role they need access to student records it is then within FERPA regulations for an institution to grant access. According to Jim Farmer, Coordinator for Scholarly Systems Group at Georgetown University, universities outsourcing e-learning systems, for example Blackboard or Moodle, are on the rise. There seems to be an increased demand for distance learning courses and in times of economic hardship this may be an untapped source of revenue for some institutions (Farmer, 2007, pg. 1).

Direct Control

Once an institution has determined that the contractor functions as a "school official" they then must adhere to the *direct control* regulation. The *direct control* statue states that "outside parties that provide institutional services or functions as 'school officials'... do not maintain, use, or re-disclose education records except as directed by the agency or institution that disclosed the information" (p. 74816). The report suggests that in order to ensure a clear understanding between both parties that the institution clearly state the contractor's responsibilities in a written contract. This does not mean that the institution has direct control over the contracting party's overall operations rather only in regards to the use of student records.

Protection of Records by Outside Parties Serving as School Officials

According to the report, it is the responsibility of the institution to "ensure that an outside party providing institutional services or functions does not use or allow access to education records except in strict accordance with the requirements established by the educational agency or institution that disclose the information (p. 74816). FERPA does not however, specifically outline how individual institutions should comply with this regulation in order to ensure the flexibility needed to best meet the institutions' needs; it does suggest periodical training through presentations and conferences. It is important to note that institutions can implement a policy to

complete background checks and fingerprinting to those with access to student records through the outsourced group however, at this time there is no authority under FERPA to have them federally mandated.

Control of Access to Education Records by School Officials

As institutions are more frequently utilizing technology for student record storage more "school officials" could potentially have access to those records. The report clarifies that even if someone is considered a "school official" that does not grant them access to any and all records; they must have a legitimate educational interest to access that particular record. An institution must therefore create a standard of "reasonable methods" to ensure there are controls in place to maintain this standard. There are no set standards in place for this requirement allowing institutions to create a system that works best for their needs (p. 74816-74817).

When outsourcing technology systems which contain student records it is imperative that an institution pay special attention to the control of access parameters within the contract. These should include security precautions related to IT in addition to who has access. President of Ohio University, Roderick McDavis, described how an IT crisis affected his university in a 2008 article. According to McDavis in 2006 he was alerted by the FBI that certain files from the Technology Transfer Department had been compromised; some of these files contained social security numbers related to parking permits. Believing it was an isolated incident McDavis was shocked to discover that the hackers had infiltrated multiple other university systems as well including alumni records, and records from the server that supported their student health center. What resulted was distrust from the university community, fearful that their personal information was no longer safe. In order to re-gain trust and to avoid similar situations in the future a consulting group was brought in to assess the situation. One suggestion resulting from the assessment was to re-evaluate their current outsourcing as it "was not a good option for the future." McDavis closed the article by suggesting that universities pay more attention to IT security issues as hacking incidents are on the rise in higher education (McDavis, 2008, p. 1-3).

If your institution finds itself in a similar situation like the University of Ohio there may be legal ramifications. According to the 2008 article "The Law, Digitally Speaking" 38 states and the District of Columbia

have laws that require institutions to notify people whose records have been involved in a security breach. There are also proposals for similar laws at the federal level. These laws may vary depending upon the state as to what constitutes a breach such as to only include medical and health care data or social security numbers. In addition to notifications there may also be fines involved; misuse of credit card information seems to be the most frequently fined for universities. Depending upon the state a sanction for misuse of credit card information may result in loss of merchant status. In the future universities may also be required to provide financial remedies to those persons who have been affected by a breach (Cate, McDonald, Mitrano, 2008, p. 1).

Proactive Versus Reactive

In conclusion there are many precautions a university can take to avoid potential IT crises related to contracted technology. Beth Cate encourages all universities to implement continuing assessments of privacy and security. The team to complete the assessment should consist of members from the units who use the information as well as "information privacy and security, legal counsel, risk management, internal audit, purchasing and contracting (particularly to deal with outsourcing issues), human resources, and academic personnel, among others"(Cate, McDonald, Mitrano, p.2). Also, contract agreements should be reviewed frequently to make sure that the records are being used in the way intended and the university retains its rights to the information at all times (Cate, McDonald, Mitrano, p.4).

Outsourcing technology has the potential to meet students' needs more cost effectively and to provide additional services that an individual institution could not afford. One should be cautious however, to maintain stringent privacy and security policies to ensure students' privacy. As the field of technology and the legal parameters related continue to evolve it will be imperative to stay informed of the most current information.

Resources

Cate, B., McDonald, S., Mitrano, T. (2008). *The Law, Digitally Speaking, 54* (30), B14.

Farmer, Tim. (2007, August). *Lessons from Blackboard?.* What Michael Feldstein is Learning About Online Learning… Online. Retrieved April 25, 2009, from http://mfeldstein.com/lessons-from-blackboard/.

Federal Register. (2008). *FERPA Rules and Regulations, 73*(237), 9-14.

McDavis, Roderick. (2008). *What Ohio U. Learned From a Major IT Crisis. 54* (30), B5.