Campus Legal Advisor

Interpreting the Law for Higher Education Administrators

VOLUME 16, ISSUE 8 APRIL 2016

SNAPSHOTS

LEGAL BRIEFS

School district bans sharing of disciplinary records; and more. **Page 2**

COMPLIANCE

Review 8 preparation steps to manage involvement of attorney, non-attorney advocates in your student conduct process. **Pages 4–5**

LAWSUITS & RULINGS

Review summaries of court cases and agency rulings. **Pages 7–14**

YOU BE THE JUDGE

Was openly gay student-council president entitled to damages for defamation? See if you can guess how the court ruled in this month's highlighted legal case. **Page 15**

QUICK STUDY

Learn how the courts have ruled in recent cases involving employment termination. **Page 16**

Training Tools

Balance institutional mission, values with free speech rights on your campus

By Claudine McCarthy, Co-Editor

ORLANDO, FLA. — Burgeoning with an influx of bright young minds and seasoned experts constantly developing new ideas and expanding knowledge, the college campus seems like the ideal environment for fostering free speech.

Even so, higher ed officials often find it challenging to embrace free speech while also keeping the peace on their campuses, whether that means dealing with hurt feelings or interference with their day-to-day operations.

It is possible to find ways to balance your institutional mission and values with fostering an environment that encourages free speech — even for those students whose speech you might find distasteful. That's according to Neal Hutchens, J.D., Ph.D., associate professor of higher education and affiliate law

Continued on page 3.

Of Counsel

Learn the 5 keys to boosting effectiveness of your cybersecurity program

By Stephen A. Grossman, Esq., and Priya Roy, Esq.

Colleges and universities are a treasure trove of information for hackers, from intellectual property rights and research data collection to student and staff financial information and Social Security numbers.

Indeed, what makes colleges and universities such remarkable laboratories of innovation and learning also renders them fruitful targets for hackers. Moreover, colleges and universities are particularly susceptible because they're often deeply decentralized and function in silos — each department containing disparate information-processing protocols and internal cultures of data-sharing.

This concern isn't lost on the U.S. Department of Education, which highlighted

Continued on page 6.

DOI: 10.1002/cala

JOSSEY-BASS™
A Wiley Brand

Continued from page 1

the obligation of colleges and universities to protect data and student information in a "Dear Colleague Letter." The ED's letter centered on the security of financial aid information and third-party handling and access to such information. However, there's no doubt the ED expects institutions to develop and implement comprehensive campuswide cybersecurity practices.

Unfortunately, you won't find a stand-alone policy or program that works for all colleges and universities. Instead, to address your cybersecurity needs you'll have to start with established policies and procedures and invest in sophisticated technical solutions.

And policies serve as only one piece of the solution. The implementation of your policies along with smoothly running processes and operations is the true test of whether your institution is prepared to handle a cybersecurity attack and whether your cyber program complies with the ED's mandate.

Consider these 5 keys to help ensure your institution has an effective cybersecurity program:

1 Classify information and identify your risks. A cybersecurity program begins with classifying the data that comes into your institution and leaves your institution. For universities, that could include intellectual property, proprietary research, student information (such as Social Security numbers, health records and financial information) and employee data. Without an inventory of data and how it's used, shared and stored, risk mitigation and security become impossible. Appropriate staff members must also understand the statutes that govern and impose special requirements over your institution's most sensitive data. For instance, student education records must be treated and retained according to the dictates of the Family Educational Rights and Privacy Act. Similarly, if you issue student debit cards or cash cards for use at dining halls, you may be subject to the strictures of the Gramm-Leach-Bliley Act.

2 Develop a centralized cybersecurity position. Given the decentralized nature of colleges and universities, the development of a centralized position responsible for your institution's cybersecurity program must become a priority. The person in this position should have the authority to delegate and manage these operations as well as develop a cross-functional team to support the program.

3 Scrutinize third-party vendors. The ED letter made it clear that higher ed institutions are responsible for data breaches caused by third-party vendors. That's why colleges and universities must ensure that vendors meet the institution's own security standards and communicate and handle data incidents and breaches in accordance with the statutes governing the institution's own conduct. In other words, because FERPA applies to the school, it also applies to vendors handling FERPA-covered records. You can mitigate this risk by limiting third-party vendors' access to only data that falls within the nature and scope of the third-party contract.

Taking inventory of your third-party vendors and determining the levels of access to secure data is a vital first step in assessing your data-security program. Third-party vendors might oversee your cloud-computing operations or email platform. And researchers might host data from study results on servers hosted by third-party vendors. Scrutinizing your third-party vendor data-security responsibilities is a critical part of your data-security program.

4 Provide training to staff members. All employees of a college or university are responsible for data security. To that end, it's imperative that staff members, even those outside the internal response team, receive periodic training regarding security protocols and steps they can take to keep institutional and student data secure. In fact, the majority of data-security incidents are caused by employee mistakes, failure to follow protocol, and even purposeful misuse.

5 Monitor security systems and practice data-breach responses. Accept the premise that a data incident or breach will happen. In light of that, all cybersecurity programs must include regular monitoring and testing. Data breaches are stressful and can be extremely chaotic, from containing the damage to determining the root cause of the actual breach. It's critical for your systems and protocols to run seamlessly when the inevitable happens. Testing can help alleviate some stress and identify vulnerability gaps. Although no data-breach response plan will go perfectly, routine practice will help your institution be as prepared as possible when an incident does strike your campus. ■

About the author

Stephen A. Grossman, Esq., and Priya Roy, Esq., are attorneys with Montgomery McCracken Walker & Rhoads. Grossman serves as chair of the firm's data privacy and cybersecurity practice. Roy focuses her work in the areas of higher education and is a member of the firm's data privacy and cybersecurity practice. Both serve as editors of the firm's Data Privacy Alert blog (*http://privacyblog.mmwr.com*), which focuses on data privacy and cybersecurity issues. ■

DOI 10.1002/cala