IRON MOUNTAIN®
GOVERNMENT SOLUTIONS

PROTECTING & ENSURING STUDENT PRIVACY

Properly managing records and avoiding cyberattacks requires an information lifecycle approach. Mary Ellen Buzzelli, Director of SLED Strategy for Iron Mountain Government Solutions, outlines the key steps you should take to protect student privacy.

A faculty member at a public university felt the pressure to protect student privacy when she inadvertently posted a video on her public Instagram page that revealed several of her students' course grades. The video, which was meant to discuss the changing weather, quickly panned over the teacher's computer screen, revealing the grades before showing the sky. Although this was clearly an accident, it brings into question the issue of student privacy.

Another main concern for higher education institutions about student privacy is the ever- increasing threat of cyber- and ransomware attacks. The COVID-19 pandemic made cybersecurity more challenging, as highlighted in the results of Educause QuickPoll from last year. "More than half of respondents reported that nine of the 15 tasks we tracked became at least a little more difficult, and about one-fifth of respondents felt that five of the tasks were now difficult or very difficult indeed: special projects or initiatives, data loss prevention, vulnerability scanning, monitoring privacy and policy enforcement," the QuickPoll noted.

This is why the U.S. government places a priority on student privacy and accessibility. For example, the Family Educational Rights and Privacy Act, or FERPA, a federal law that protects the privacy of student education records, applies to all colleges and universities that receive funds under an applicable program of the U.S. Department of Education. It's essentially the education market's version of the Health Insurance Portability and Accountability Act. In terms of accessibility, the Individuals With Disabilities Education Act (IDEA) is a law that makes public education available to eligible children with disabilities throughout the nation.

As colleges and universities work hard to protect and ensure the privacy of records associated with both laws, they must consider their entire information management program. That means they should shepherd student records and information throughout a life cycle, beginning when a record is created and continuing through its usage, storage, retrieval and maintenance. At the final stage of the life cycle is disposition and destruction or permanent retention of material in accordance with FERPA or applicable state laws for record retention.

Properly managing records and the information life cycle is the best enabler of cybersecurity as well. This helps a higher education institution determine where its information/data resides, their value and how to effectively manage them throughout the life cycle.

The benefits of such a life-cycle approach are significant and include:

Reduction of stored records and storage costs

Mitigated exposure from data breaches

Enhanced ability to control record volume

Improved speed and accuracy of record retrieval

Key Aspects of the Life Cycle

How can you and your institution best manage current and future students' records and data across such a life cycle? Depending on the size of the institution, the people involved in this type of a program can vary significantly -- from the records manager and the head of the student data oversight committee to the general counsel and the chief data officer. Colleges and universities need to identify the roles and responsibilities to have a successful program.

The process can be overwhelming at times, but if you focus on the following steps, you will be in a much better place moving forward.

Establish a framework. Developing an information management framework is the first step in the process. It enables colleges and universities to address requirements associated with risk management, retention and compliance early on, providing added control over the information from the point of creating a record to its final disposition.

You should first inventory all your institutional data and develop an information map of the databases related to your institution's systems, applications and repositories; where those databases are located; and who is responsible for managing them. That will give you a better understanding of your college or university's information, systems and records -- allowing you to identify sensitive information, monitor the use of assets and gain analytical insights. Specifically, an effective information management framework requires the following steps:

1. **Organize.** You should establish the parameters of the information management program by developing a documented, multiyear strategic plan that provides the tools and resources needed to meet program objectives for all types of records. That includes defining and assigning roles and responsibilities to ensure that everyone involved in the program has set expectations regarding their responsibilities for both physical and digital records. For example, the records manager might be responsible for establishing the day-to-day access process -- how the staff requests specific records, the duration those records can be "checked out" or what metadata might need to be incorporated into digital records. A chief privacy officer, in contrast, might be responsible for setting the retention policies or ensuring the institution is in alignment with FERPA.

2. **Assess.** Next, conduct a comprehensive assessment of the needs, capabilities and obligations that form the foundation of your information management program. To accomplish that, your institution needs to evaluate existing programs (if any), conduct a thorough records inventory and classify records dependent on function -- such as financial aid forms, personal health records, grading reports and the like.

3. **Develop.** Creating an actionable retention schedule and formalized policies is the next component for establishing a credible, consistent and compliant information management program. Although each state maintains different rules for data classification/sensitivity, storage methods, length of retention, reporting requirements and approved methods of destruction, colleges and universities should establish a schedule that meets the needs of their students. For instance, records associated with student housing might only need to be stored for the duration of the time a student is enrolled, while grading records might have to be stored for decades.

4. **Implement.** Properly implementing the information management program is of utmost importance. To be effective, you should conduct the rollout in a phased approach, with the IT department integrated into the process. As part of this, you should complete the legacy inventory, as well as create and execute a communications plan that includes proper training for all involved. This plan should then be communicated to anyone who is responsible for storing, managing or accessing records. From financial aid to admissions, all personnel must understand the policies put in place to protect student privacy.

5. **Manage.** After you've completed the implementation, it's time to plan and budget resources for the continued maintenance, enhancement and enforcement of the program. That includes defining and tracking key metrics -- such as are you meeting the desired turnaround time for record requests, or have you properly disposed of those records that have hit their retention requirements -- managing the security, accessibility and integrity of data; maintaining ongoing training and internal communication; and ensuring appropriate oversight.

6. **Audit.** You should continually review your information management program to ensure that your institution remains compliant and meets performance measures. That means identifying areas where the program might not be working and putting improvements in place to make it more effective. An audit, for example, may reveal that you are preserving data you no longer need. Destroying unneeded records can free up space and help to save on storage costs.

Implement access controls. Once you've put a framework in place, you'll need to protect the data and information by enforcing access controls to it. Utilizing secure, off-site storage options can be a creative and cost-saving solution. Suitable facilities will provide physical security capabilities and should feature controls like access-controlled security cages and other internal measures; controlled parking, loading dock access and external safeguards; and fire, water, temperature and other environmental protections. Such off-site facilities help to limit risks associated with lost, damaged or stolen records, while enhancing records-retention practices and making information readily accessible.

Maintain a chain of custody. Maintaining a strong chain of custody for your information and data, from ingestion and cataloging to subsequent preservation and distribution, is the next challenge. A chain of custody is the complete, documented, chronological history of the possession and handling of a piece of information or a record. It includes a set of procedures that assigns a distinct identifier to each asset in order to enable it to be tracked constantly, no matter where it is along its life cycle. Whenever an item is retrieved, accessed or distributed, this information goes into the permanent, unique record for that item, allowing a college or university to have real-time knowledge of a record's location and status. Having a strict chain-of-custody process helps prevent the loss or damage of a record, as well as more effectively protects student privacy.

Manage records and information over the entire cycle. Educational institutions should develop an enterprise strategy that applies to all digital and physical information, both current and future. That means establishing long-term processes for inbound and outbound record storage and retrieval services; archiving and preservation; pickup of newly created records; digitization of records; and disposition requirements including accession, archiving or destruction of documents.

As the focus on student privacy continues to be one of the most important, as well as challenging, issues today, educational institutions must focus more time and resources on information management. And that starts with protecting the myriad student records generated each day on your campus. By taking a more detailed and managed approach, one that considers the entire information life cycle, your institution will be in a much better position to do just that.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world.
Visit the company website at www.ironmountain.com for more information.