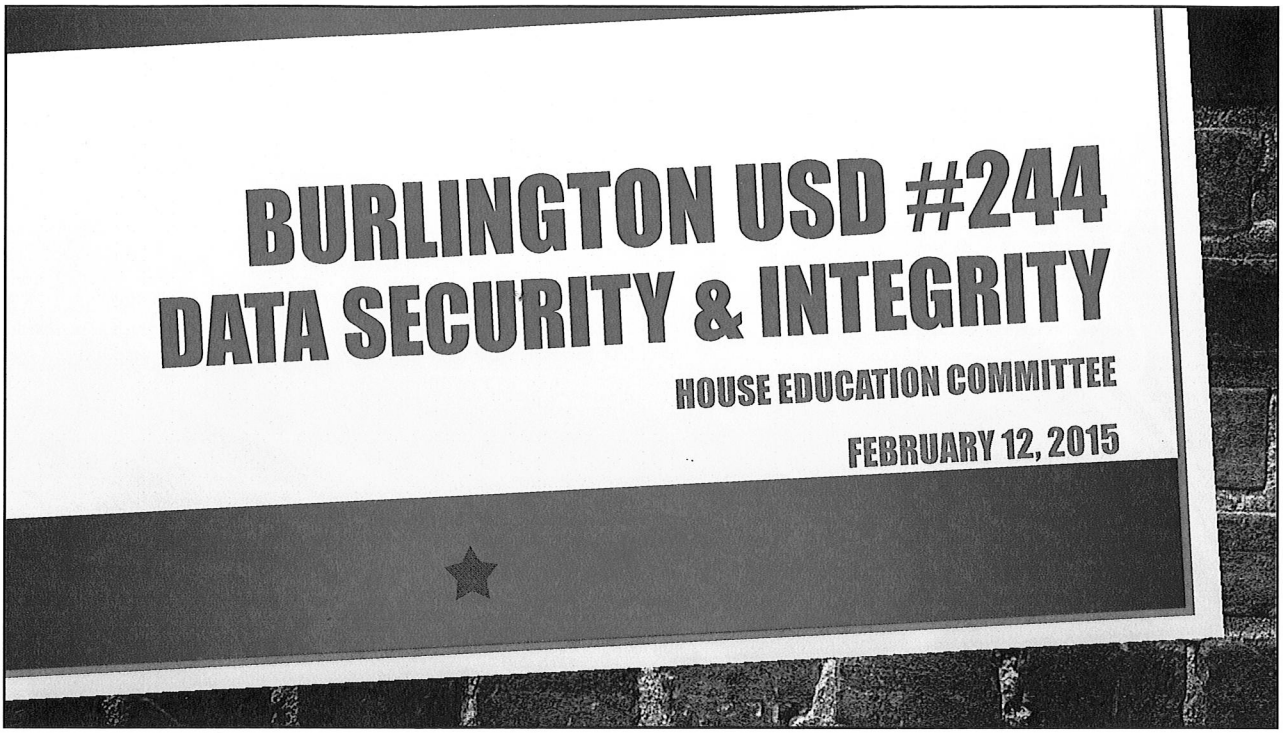


OVERVIEW OF PROCESS

- Physical Control & Integrity of Data
- Access Control to Data & Student Information
- Contingency Planning & Recovery

PHYSICAL CONTROL & INTEGRITY

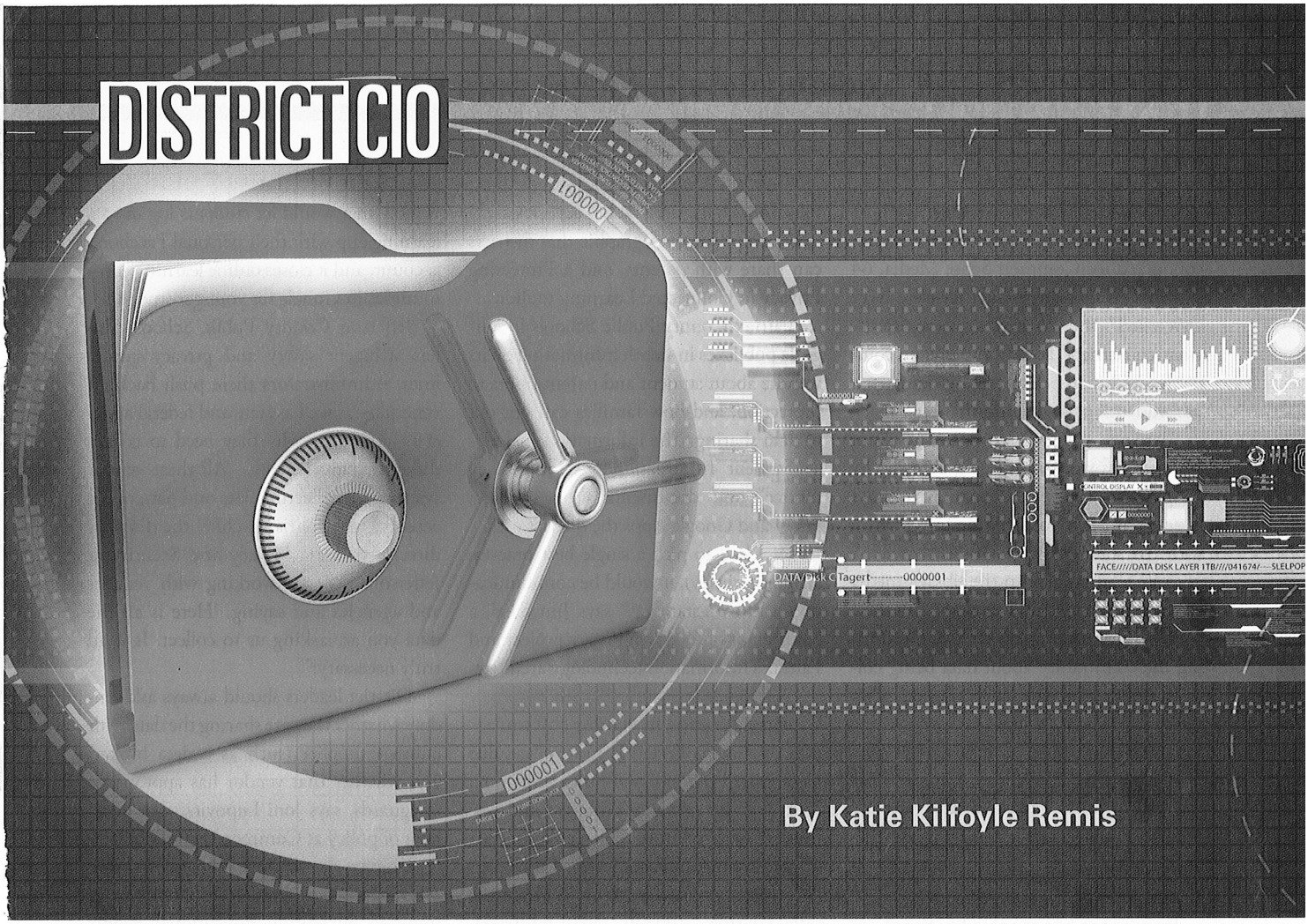
- Device Protection (Tablet, Laptop, Desktop & Server)
  - Virus, Malware, Botnets, SpyWare, Zero-Day Attacks
  - Both Device & USB (high risk for schools)
  - Routine Scans & Updates (both push and pull ability)
- Electronic Mail Protection
  - Sits outside the firewall for both Staff & Student e-mail accounts
  - Protects SPAM, Virus & Denial of Service Attacks
- Internet Protection
  - NextGeneration Firewall with AntiVirus, Intrusion Prevention, RED, Content Filtering & More
  - Physical Separation between Database Servers & Web Servers (DMZ & Different Servers)

ACCESS CONTROL TO DATA & STUDENT INFORMATION

- Focus on Both Device Level & User Level Access
- Evaluate Contracts & Data Integrity Plans of 3rd Party Educational Companies
- Very hesitant to use Cloud-Based services.
  - WE are responsible for our data!! Build our own cloud. Device Synch.
- Protect Students in electronic mail and other communications. (Special Needs)
- Compliance with FERPA, COPPA and PPRA.

CONTINGENCY PLANNING & DATA RECOVERY

- Backup System
  - Lessons from Greensburg & Chapman
  - Multi-Campus (Storage Based on 1 Campus. Tape Based on 1 Campus.)
  - Quarterly Tape Rotation to a Secure off-side location. (County EEOC center)
  - Use SAME Hardware & Software System as County Courthouse.
  - Partnerships in Community Networking
- Contingency Planning
  - Physical Server Recovery
  - Remote Site Recovery & Operations (paychecks & financial information)



By Katie Kilfoyle Remis

LOCKING DOWN STUDENT DATA

Keeping information out of the wrong hands requires leadership, diligence and collaboration

The increasing shift to online learning and collaboration has created new concerns around student privacy. Keeping data as secure in the cloud as it would be in a locked file cabinet requires communication, diligence and strong policies.

"Privacy is not a new issue but it certainly has risen to the top in part because so much of our lives are moving into the internet and the cloud," says Bob Moore, director of CoSN's Protecting Privacy in Connected Learning project. "We had days when we thought, 'Who would hack student information?' But the reality is that it can be used for identity theft, even later in a student's life."

In January, President Obama proposed legislation that would prohibit companies from selling student data to third-party companies for noneducational purposes. This comes a year after Jefferson County Public Schools in Colorado stopped using inBloom, a nonprofit corporation that warehoused and managed student data, when community members raised concerns about privacy. An outcry from other districts and critics

V+S+C
DAmag.me/LockData

led inBloom to shut its doors last April.

And in a national survey of 800 parents conducted for Common Sense Media, 64 percent of respondents said they were "very concerned" and 26 percent were "somewhat concerned" about how private companies with non-educational interests can use students' personal information.

"Parents get very concerned about whether information is being accessed by people who don't need to know it," says Moore. "Is the school sharing information with the state or other entities that don't need it? Can an aide in the library media center access a student's grades?"

Districts can ease concerns by informing the community about data being collected, why they are collecting it, what they do with it, and who has access. CoSN created a privacy infographic that districts can share with parents, and a Protecting Privacy in Connected Learning toolkit.

Fairfax County Public Schools in Virginia publishes in-depth information on its website about student and parent rights to protection, and how families can opt out of data sharing. The information includes a "Student Information System Privacy Notice" and documents about internet safety and Google Apps the district uses.

"If I had to pick a single best practice (around privacy), it would be communication and transparency," says Jim Siegl, a co-director of CoSN's privacy project and Fairfax's information technology architect.

Closing the gaps in vendor software

Data is being collected in more places due to increased use of cloud-hosted software. This includes subscription-based and free instructional software, Google Apps, document sharing, library ebooks, online tests and emergency notifications. Without the right controls, students' email addresses, passwords, assessment data, patterns of activity and classroom performance could be viewed by the wrong people.

A study from Fordham University, released in December 2013, found that fewer than 25 percent of cloud service agreements specify how student information can be used, and fewer than 7 percent of the contracts restrict the sale or the marketing of student information.

In response, Fairfax County schools developed a rigorous checklist to ensure that student privacy is protected and that software is appropriate (see sidebar to left). "If an application doesn't make it through our red flags, it's pretty easy to find another one that does the same thing with better privacy," said Siegl. "If it's a significant app, our experience has been that when we reach out to vendors, most are responsive to making it more secure. And it's not always a case of whether the app is good or bad; a lot depends on how you configure it to make it more secure."

For example, the district disables connectors that would let students log in to a learning app with their personal Facebook account, and it closes online learning communities in Google for younger students.

Jefferson County Public Schools also has stringent safety and privacy guidelines. Administrators there push back on vendors—as well as state and federal agencies—to justify why they need to collect different data elements. "All these vendor systems are collecting data and patterns of activity," says Chris Paschke, the district's director of Data Privacy and Security at Jefferson. "We are working with vendors and agencies and saying, 'Here is all the data you are asking us to collect. Is it all truly necessary?'"

District leaders should always ask vendors whether they are sharing the data with another supplier (such as a data broker) and whether that vendor has appropriate safeguards, says Joni Lupovitz, vice president of policy at Common Sense Media.

Conversely, vendors need to be aware of a school's requirements, especially those imposed by Family Educational Rights and Privacy Act (FERPA). Vendors must build compliance into their technologies, contracts, and business processes. "Vendors have to understand that it's the district's data, not theirs—it's for the district's benefit, not theirs," says Steven J. McDonald, general counsel at the Rhode Island School of Design and a leading specialist on federal education privacy law. "Vendors can filter it for spam and viruses. They can data-mine an assessment program to evaluate a response and tailor the next question. But they can't data-mine it for their own advantage."

Last October, The Future of Privacy Forum and the Software & Information Industry Association announced a K12 service providers pledge (http://DAmag.me/4sm2qx) with a list of commitments regarding the collection, maintenance and use of student personally identifiable information, or PII. The commitments include enforcing strict limits on data retention and not changing privacy policies without proper notice.

Assessing apps

Staff at Fairfax County Public Schools in Virginia assess 200 to 250 pieces of software each year. Its process has received national recognition from the U.S. Department of Education. At a minimum, online software used by Fairfax County schools must meet the following criteria:

- Well-defined privacy policies that apply to the app and website
- Encryption of any student data that's transmitted
- Age-appropriate tools, software and ads
- Moderated and secured online communities
- Restricting students from logging in through Facebook or public accounts
- Not capturing information unnecessary to the app's functions

Equally diligent is Jefferson County Public Schools in Colorado, which measures online software against 30 different standards, including how much data security training a vendor gives its employees and whether they've had background checks.

Free apps come with a price

A great concern for districts are so-called "clickwrap agreements," where end users, like teachers, click an "OK," "I Accept," or "I Agree" button to activate a free app that has not been vetted by the district. Teachers likely haven't considered where and how data collected by the app might eventually be used.

"Free apps are not free," says McDonald. "There may not be an exchange of money, but it is usually an exchange of privacy and that's where districts have to be careful. Someone who clicks on that agreement is acting on behalf of the district and it could be a recipe for a FERPA violation."

Signing a fee-based contract with a vendor that's new to the K12 market and unfamiliar with FERPA restrictions is another concern, McDonald says. Teachers at Fairfax County schools can use software only if it has been vetted by the district.

Jefferson County schools created a training video to help educate teachers on ways to identify free apps that are secure. District technology staff are reviewing more than 600 free apps that teachers use to see if they have well-defined user agreements and if there are other security issues.

The decision to centralize and vet software varies from district to district, depending on the school community's culture and expectations. But district leaders need to clearly define teachers' roles and responsibilities for protecting student data regardless of how apps are acquired, says Geoffrey H. Fletcher, deputy executive director at SETDA.

And there is no shortage of resources and regulations. At a minimum, districts should be compliant with FERPA, the Children's Online Privacy Protection Act (COPPA) and the Protection of Pupil Rights Amendment (PPRA). But even then, some questions remain.

For example, FERPA applies to personal information, but that information is not maintained or under the direct control of the school when it is a consumer service, says Siegl. A typical example is when a student uses a journal on a blogging platform.

So, in the absence of any clear laws, most schools include digital citizenship in their curriculum and use best practices and common sense to deal with such scenarios. They may direct students not to use their last names and to obtain parental permission. Some areas of technology are outside the scope of what FERPA covers and remain gray areas for now, Siegl says.

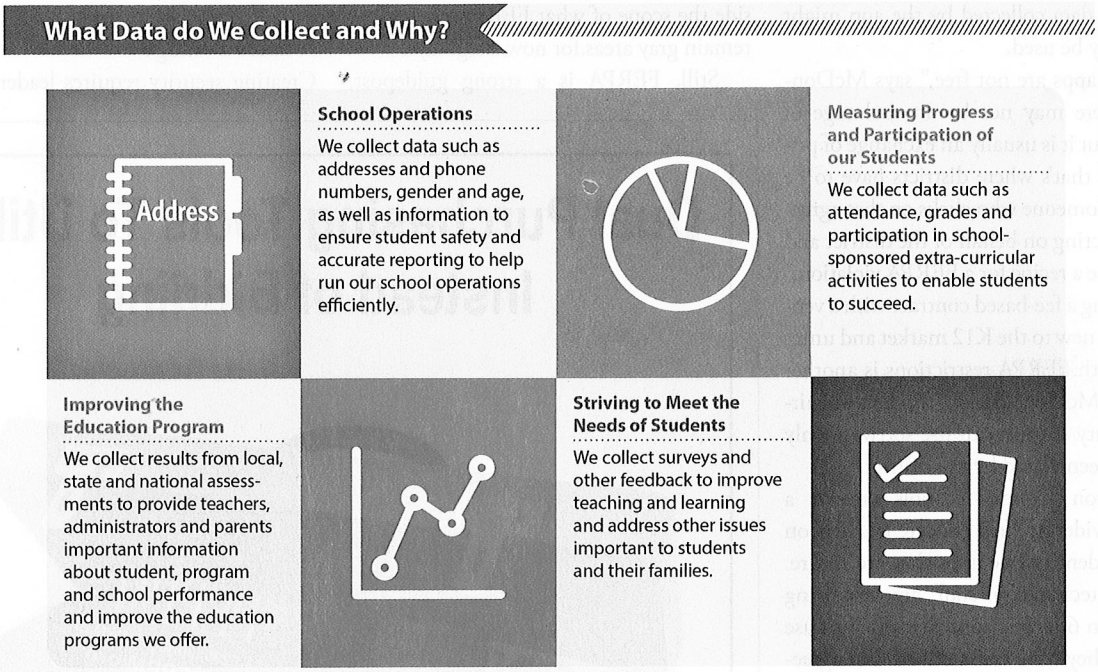
Still, FERPA is a strong guidepost, McDonald says. "The definition of 'education record' is broad and it covers everything directly related to a student and maintained by an education institution," he says. It ranges from disciplinary records, disability accommodations, athletics and a student's bus route.

It takes a village

Creating security requires leadership and

A toolkit

The Protecting Privacy in Connected Learning toolkit is an in-depth, step-by-step guide to navigating four major federal laws. The revised toolkit covers the Family Education Rights and Privacy Act (FERPA); Children's Online Privacy Protection Act (COPPA); Health Insurance Portability & Accountability Act (HIPAA); Protecting Pupil Rights Amendment (PPRA); and related privacy issues. The toolkit addresses FERPA and COPPA compliance issues as well as suggested practices that reach beyond compliance; it also includes definitions, checklists, examples and key questions to ask.



Source: CoSN

the involvement of staff from technology, academics, the business office and legal. Districtwide collaboration is also a necessity. "But ultimately, it comes down to the superintendent and the board of education. Privacy and compliance are very clearly policy issues," says Moore.

At Fairfax, software first goes through a curriculum review and then to the technology department for assessment. Additionally, a governance group comprising instructional and technology staff meets regularly to discuss privacy and data.

At Jefferson County, privacy is part of a larger focus on quality. The district formed a data governance structure in 2013 that includes three departments that work closely together: Ed Tech Support & Data Quality, Educational Research & Design, and Student Data & Assessment. The district added two new analyst positions and created a data privacy committee with 10 parents and 10 staff members who meet monthly.

Together, their data initiatives include:

- Identify the data that is being collected intentionally and unintentionally.
- Determine which data is necessary, and stop collecting unnecessary data.
- Measure online software to ensure it's technically and contractually secure.
- Raise awareness about data collection
- Scan for technical vulnerability, and establish strong login management.
- Classify data being collected and establish processes for each category of handling, retaining and sunsetting.

Curtis Lee, director of Jefferson County's Ed Tech Support & Data Quality department, recognizes the scope of Jefferson County's efforts is broader than most districts can support. "Data quality intersects with security and privacy," says Lee. Documenting solid processes for data control helps alleviate privacy concerns and bolsters community confidence that the district's policies are based on good data.

And Jefferson County's Paschke adds that privacy issues need to be addressed consistently at the state and federal levels. "Right now we are doing a lot of good work, but we are also defining the way that we manage risk and privacy," says Paschke, "and by definition we are inheriting risk by creating the process." **DA**

For a list of resources go to: http://DAmag.me/LockData

Katie Kilfoyle Remis is a freelance writer based in upstate New York.