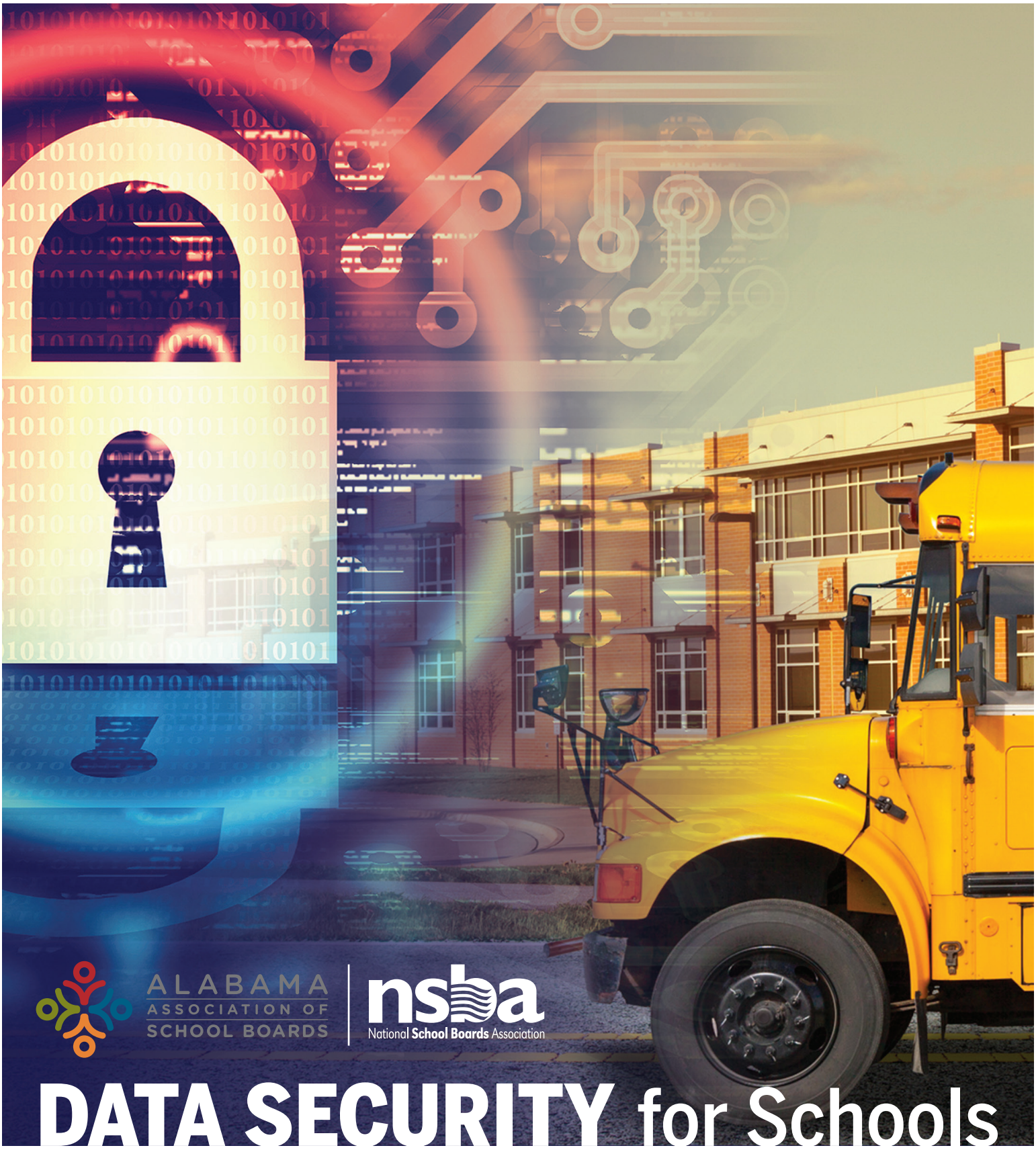

ALABAMA ASSOCIATION OF SCHOOL BOARDS

nsba National School Boards Association

DATA SECURITY for Schools

A Legal and Policy Guide for School Boards

Christine N. Czuprynski, McDonald Hopkins LLC 2019

Table of Contents

Data Security for Schools

Introduction

You have seen the headlines: Social Security numbers lost. Credit card numbers stolen. Email addresses accessed and misused. Data breach events affect thousands, hundreds of thousands, and sometimes millions of people. Most often, the data breaches making news are suffered by companies like Target and Equifax, or institutions like the University of Maryland and the U.S. Government. But local school districts are no less susceptible to data breaches than these high-profile entities. And they may face similar consequences: regulatory scrutiny, private lawsuits, and distrust of stakeholders like parents, students, teachers, or administrators.

You can help prevent data breaches and mitigate their effects through strong data security practices. This guide is designed to help you identify such practices as you develop or revise your school district's approach to data security. We will discuss the importance of data security in school districts and its intersection with data privacy and data governance, and describe legal requirements and best practices for school districts in the event of a data security breach, including what kinds of remediation steps are necessary.

Data *privacy* and data *security* are often thought of as one and the same, as solid data security measures are aimed at protecting the privacy of the data. In the context of the day-to-day operations of a school district, however, data security and privacy are different.

Data privacy relates to the collection and use of personal information of both students and staff. Schools collect student names, addresses, dates of birth, Social Security numbers, demographic, contact, academic, and other identifying information for inclusion in each student's record. Schools also collect employees' personal information, compiled into each employee's personnel record. Schools monitor use of such data carefully — data privacy would include an assessment, for example, of whether student names and email addresses should be shared with a third-party vendor, which then uses that information to send marketing materials to the students. Data privacy also can include how student records are shared with the student, his or her parent or guardian, teachers and other school staff, and other third parties, consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA) and state laws.[1] And data privacy includes how school districts handle employee data, under applicable federal and state laws.

Data security describes the protections in place to prevent unauthorized access to or acquisition of personal student and staff information. A school district's data security measures might include keeping student and staff personal data in locked filing cabinets, and limiting access to those filing cabinets to people within the school district who need that data in order to do their jobs. Data security also includes using encryption when transmitting personal data electronically, requiring school district employees to use passwords to access files containing personal data, and installing software that detects intruders in the computer network.

Consider an educational application, digital learning tool, or other online educational program used by a classroom teacher that collects student data. Data privacy is the concept covering the collection and use of that data, while data security covers the steps taken to prevent that data from being lost or stolen. School districts across the country are grappling with how to balance the need and convenience of this technology with the data privacy and security concerns of students, parents, educators, and the district itself.[2]

NSBA's Guide *DATA IN THE CLOUD: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era*[3] addresses the issues you should be thinking about regarding data privacy. It is a companion to this guide, which aims to do the same for data security. Neither guide is intended as a substitute for appropriate legal counsel. School boards are well served by seeking the advice of a school lawyer who is a member of the NSBA Council of School Attorneys (COSA), as well as your state school boards association, when designing and identifying polices around the issues presented here and by digital data concerns generally.

With this background, we turn to some Frequently Asked Questions (FAQs) about data security for schools.

1 What data security risks do school districts face?

It is generally accepted that data breaches are an inevitable part of data collection. Information—especially personal information—is valuable. Credit card and bank account numbers provide the most direct access to financial accounts, which can be exploited for any number of reasons. Social Security numbers are the "keys to the kingdom" for those people who want to commit identity theft; they can be used to obtain new lines of credit and access existing bank accounts. Hackers are interested in accessing systems that store this kind of personal information.

Leaving data unprotected is akin to leaving one's wallet on the front seat of an unlocked car. School districts face very real security threats because they collect, use, maintain, disclose, and discard valuable personal information about students, teachers, and employees. The question you face as school district leaders is not "what should we do if we get breached?" but "what should we do when we get breached?" To prepare for the inevitable data breach, you should understand the specific risks school districts face.

Areas of risk[4] generally include:

- **Theft** — Deliberate attacks on systems and individuals who have access to sensitive data. Such attacks can cause more harm than inadvertent exposure. Examples: Hacking of district human resource records to obtain employee information, including Social Security numbers; hacking to install malware using encryption that holds district data hostage until a ransom is paid.
- **Loss** — Inadvertent exposure due to the loss of media. Examples: District backup tapes or paper files are misplaced on their way to a storage facility; laptops are left behind at airports or in taxis.
- **Neglect** — Insufficiently protected data. Examples: Outdated district computers or hard drives are sold or recycled without properly erasing district data, making the information retrievable by anyone with just a few cheap tools; data sits on media that is not adequately protected with a strong password or with encryption, leaving it vulnerable to a hacker or thief.
- **Insecure Practices** — Insufficiently cautious collecting, storing, sending, encrypting, finding, and removing data. Example: Individual student achievement data is transmitted via unsecured email or public wireless networks.

A. How do breaches occur?

Computer system intrusions can range from highly sophisticated to highly simplistic. Hackers are able to use

their skills to infiltrate complicated networks protected by robust security protocols, but many attacks are much simpler. A very common example of a simple attack is a phishing email. Hackers use phishing emails to trick individuals into voluntarily providing access to their personal information, usually by masquerading as a legitimate sender. Hackers also use phishing emails to gain access to computer systems; once in, the hacker can find where valuable information is stored. Phishing emails sometimes include poor grammar and spelling, and a sense of urgency, though these emails are getting more sophisticated and harder to spot. Below is an example of a fairly basic phishing email meant to induce an employee to click on the link and provide personal information:

To: joe.smith@acmeschools.com
From: ACMESCH00LS.com
Subject: EMAIL ACCOUNT SHUT DOWN
Date: November 12, 2017

Your Acme School District email needs to be verified to avoid De-activation

11 November 2017 **You have less than 24 hrs**

Click the button below to continue to use this service

Continue with Verification

Warning: Failure to do this will lead to suspension of your email account

Many thanks to you for considering.

Regards,
Acme School District

This example demonstrates how hackers create a sense of urgency to induce recipients to act quickly by clicking on the link and providing information before questioning the legitimacy of the email from the start. Another clue that this message is a phishing email is the "From" line. The word "schools" in the sender's email address includes zeros instead of the letter "O." There is also something slightly off about the language or wording of some of the sentences. These hallmarks of a phishing email can be hard to spot, even for seasoned information security professionals. In any setting, it is a best practice never to click on a link in an email, even if it appears to come from a trusted source, but to cut and paste the URL into your browser.

Breaches also occur as a result of honest mistakes and accidents. The wrong files are emailed or made available online. Laptops that contain personal information are left at the airport charging station. School records are forgotten on a bus after a long commute home. Sensitive documents are thrown away in a dumpster instead of being shredded. When these mistakes happen, they can sometimes be corrected without exposing individuals to any harm. Sometimes, though, enterprising thieves can gain access to sensitive data that can be exploited.

B. Have school districts been harmed by data breaches?

Yes. School districts across the country have suffered data breaches affecting students and/or staff. The Privacy Rights Clearinghouse keeps a running chronology of reported and publicized data breaches. Of the 49 data breaches it compiled on educational institutions for 2017, 2018, and the first part of 2019, eight (8) of those breaches involved school districts.[5] The breaches resulted from phishing attacks, carelessness with student records, and lost or stolen portable devices that hold data. Here are some examples:

- **December 2018** — A school district in southern California reported a breach impacting approximately 500,000 former students and some staff. The impacted information included individuals' names, addresses, and dates of birth; discipline, health, scheduling, and grade information; as well as some Social Security numbers.[6]
- **February 2018** — A New York school district may have mistakenly mailed notices to students and families in envelopes where sensitive information was viewable through the envelope's window.[7]

A data security breach often requires a school district to expend significant amounts of time, energy, and money to investigate and remediate the breach. The Ponemon Institute has found that, across the organizations it studied, the average cost to address a data breach is $150 per lost record, and the average total cost to address a breach was $3.92 million.[8]

Given this significant and very real risk of data breach, what should you do as a school district to prevent and prepare for one? Before addressing specific data security measures, a school district should plan more broadly for data governance.

2 What is data governance? Does my school district need a data governance plan?

Data governance is the body of policies and procedures that addresses how the school district's data, especially personal information, are collected, stored, used, and shared. Put simply, data governance is the overall management scheme for an organization's data. Data governance is an important step to protect against the risks outlined in FAQ #1.

A useful resource on data governance is the National Forum on Education Statistics' *Forum Guide to Education Data Privacy*.[9] It is designed as a reference document for state and local education agencies (SEAs and LEAs) in protecting the privacy and confidentiality of student data. Though the focus of the *Forum Guide* is on privacy, it provides some guidance on data governance and data security:

> In general, data governance refers to the overall management of the availability, usability, integrity, quality, and security of data (NCES 2012). By clearly outlining policies, standard procedures, responsibilities, and controls surrounding data activities at each point in the data lifecycle, a data governance program helps to ensure that information is collected, maintained, used, and disseminated in a way that protects individuals' rights to privacy, confidentiality, and security, while producing timely and accurate data. A comprehensive data governance structure will include both privacy and security policies and procedures.
>
> Data governance councils (or committees or programs) were adopted in most SEAs as the agencies were building their statewide longitudinal data systems. The growing amount of individual student data collected and stored electronically by education agencies led to greater scrutiny of data management and protection practices. Data governance programs help ensure that appropriate policies and procedures are in place to facilitate access to and use of student data while protecting student privacy. Some LEAs have also adopted data governance programs as their use of data continues to expand.[10]

The *Forum Guide* describes the crucial components of an agency's data governance program and outlines policies, standard procedures, responsibilities, and controls at every point in the data life cycle: define, collect, store and protect, use, share, and retire. It is reasonable to foresee that state and federal regulators may increasingly expect school districts, and even individual schools, to have clear, transparent and well-executed data governance programs. As the *Forum Guide* notes, this may require more cross-agency data planning.

In March 2016, the U.S. Department of Education released a Data Sharing Toolkit for Communities,[11] which attempts to clarify how FERPA may allow data-sharing, especially when student information is de-identified and aggregated, to provide wrap-around services to students. On the page entitled "FERPA Mythbusters," the toolkit notes, "Sharing group or grade-level aggregate data can help community partners provide services tailored to student needs."[12]

3 What should my school district do to safeguard the security of data?

Your school district should include policies and procedures for data security as part of its larger data governance program. Several sources offer guidance to districts on steps to take to safeguard data:

The U.S. Department of Education (ED) offers resources including a data security checklist,[13] as well as guidance on data destruction[14] and data breach.[15] At a minimum, your school district should review and consult this data security checklist as you develop policies and procedures to safeguard the security of the district's data.

Another source of guidance on data security practices is Massachusetts' stringent regulatory requirements on the subject. The Massachusetts regulation applies to every "person" who owns or licenses personal information about a Massachusetts resident, including school boards and school districts. It requires those school boards and school districts to take specific steps to protect personal data.[16] Under the Massachusetts regulations, school boards are required to develop, implement and maintain a comprehensive information security program (CISP) that:

> [C]ontains administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information.[17]

Essentially, a CISP tells school employees what risks the school district faces, and what the district should do day-to-day to protect itself from those data security risks.

Though your state may not have similar data security requirements, the Massachusetts regulations can provide helpful guidance as they parallel many of the best practices outlined by ED.[18] The following suggested data security steps combine elements of both the ED checklist and the Massachusetts CISP requirements.

A. Develop a comprehensive network map, data map and data governance plan.

The first step in protecting against a data breach is to have a clear understanding of the type of personal information being collected and used, who has access, where it is being transmitted, and how it is being discarded. The district should know: What information do we collect? Where is it stored within our systems? Who has access to it? Who can share it? How is it protected at every stage as it moves through our system? The district should also have documentation of authorized and unauthorized devices used in the computing environment.

Getting a grasp on this information will require a thorough information technology audit by either in-house or outside data security experts. ED recommends that independent assessments of data protection capabilities and procedures be performed periodically.[19]

One of the most important principles in data security is to limit the type and volume of personal information collected. A school district can not lose what it does not have. However, this can be challenging, given the myriad data that school districts are required to collect and report to state and federal agencies. This makes a school district's diligence in implementing data security measures all the more important.

B. Create employee policies and procedures that focus on security.

As part of the broader data governance plan, your district should develop policies and procedures to address data security. These are described in more detail under FAQ #4. Here is a quick overview:

- Appoint a Chief Privacy Officer (CPO). *See* FAQ #4A below for more information about CPOs.
- Develop an Incident Response Plan to contain and fix any breach that occurs.[20] *See* FAQ #4A below for more information.
- Implement an Acceptable Use Policy governing all online activity, both internally and on the internet.
- Screen and train employees, and discipline for policy violations.
- Monitor data protection capabilities and procedures periodically.

C. Protect the physical security of hard documents and implement document destruction standards once that personal information is no longer needed.

As described in FAQ #5, some states require notification of breaches in the event paper documents are lost. For that reason, your school district should secure paper files in locked file cabinets and storage facilities. Federal law contains specific directives for certain types of records. The federal Individuals with Disabilities Education Act (IDEA), for example, requires the Secretary of Education "to ensure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by State educational agencies and local educational agencies…."[21] Under document destruction regulations implemented pursuant to IDEA, personally identifiable information belonging to a child must be destroyed at the request of the parent when such information is identified by the school district as no longer needed to provide educational services to the child.[22]

D. Authenticate users who access computer systems with secure user IDs and passwords.

Your school district should limit access to sensitive data only to those who need such information to fulfill their job duties. There may be entire departments within the school district that do not need access to student or staff personal information—the custodial staff, for example. Those who are provided access to sensitive personal information should be required to use secure passwords and other methods of authentication to access it. Passwords should be complex, unique, changed often, and stored securely.

E. Employ a layered approach to system security.

Implement firewalls. Use Intrusion Detection/Prevention Systems (IDPS), which monitor systems for unauthorized use of or access to personal information. The system should be segmented properly so that if someone gets into one area, he or she does not have full access to the entire network. Intrusions into the system should be monitored and shut down as quickly as possible. Test and configure all hardware and software to ensure and optimize security. Use malware and virus protection services. Scan networks and systems on a regular basis to minimize the time of exposure to known vulnerabilities. Address how security patches will be applied to which systems at a specified time. Shut down all services and ports that are not required in the computing environment.

An issue brief from the Center for Digital Education[23] suggests a number of steps to determine where there are potential vulnerabilities, such as wireless networks, mobile devices, cloud-based services and infrastructure. It recommends three layers of security:

(1) **Administrative Controls** — Administrative security technologies limit user access to student and other data and applications. Limiting access with administrative controls is the most elemental step in cybersecurity.

(2) **Technology Controls** — Technology controls monitor on-premises, cloud-based and hosted networks, data, applications and systems for malicious activity. Many of them use data analytics techniques to track and analyze device and user behavior to prevent and detect intrusions.

(3) **Physical Controls** — Protecting physical machines and infrastructure — local computers and servers, storage media, printers, scanners, copiers and multifunction devices — is often overlooked in the rush to secure networks, applications and associated data.

F. Use encryption.

Encrypt sensitive data stored on servers or on mobile devices, such as laptops or smart phones, as well as files that are transmitted using unsecure email, over public networks or wirelessly. Personal information should be stored securely and protected during transmission.

G. Ensure that service providers implement reasonable security measures.

Even if your school district has great data security, if it works with a cloud services provider that stores school district data in an unsecure manner, you may be on the hook if and when that provider has a breach. Your school attorney member of the NSBA Council of School Attorneys has access to helpful resources on contracting with data service providers and best practices that suggest security measures that districts should require from outside vendors.

Though there is never a 100% guarantee, the security measures outlined above will put your district in a strong position to defend itself in the event of a security breach. They will not only increase a school district's protection against a security breach in the first place, but also mitigate the damages that a security breach can inflict if one does occur. For example, if a laptop containing sensitive student data is lost or stolen, the damages of that incident are mitigated if the laptop itself is encrypted. If the computer network has appropriate firewalls and an Intrusion Detection System, a hacker who is able to access the network may be walled off from the most valuable information, and his or her arrival can be detected so that he or she can be kicked out of the system quickly.

4 What kinds of data security policies and procedures should a district have in place?

A. Comprehensive Information Security Program and Chief Privacy Officer

Though creating and maintaining a CISP is only legally required for districts that collect information on Massachusetts residents, all school districts should consider implementing a CISP as a best practice.

As part of the CISP, the school district should consider appointing a Chief Privacy Officer. Some states are beginning to require such a position at the state level. For example, New York Education Law requires the appointment of a state CPO who should be "qualified by training or experience in state and federal education privacy laws and regulations, civil liberties, information technology, and information security."[24] The New York statute mandates that the appointment of a state CPO be made by the commissioner of education.[25]

Some of the state CPO's functions may include: promoting the implementation of sound information practices for privacy and security of student data or teacher or principal data; assisting the state commissioner in handling instances of data breaches as well as assisting the state commissioner in due process proceedings regarding any alleged breaches of student data or teacher or principal data; and providing assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data or teacher or principal data.[26]

New York law suggests a CPO may be given power to: (1) access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by an educational agency that relate to student data or teacher or principal data; (2) review and comment upon any department program, proposal, grant, or contract that involves the processing of student data or teacher or principal data before the commissioner begins or awards the program, proposal, grant, or contract; and (3) any other powers that the commissioner shall deem appropriate.[27]

B. Incident Response Plan

The district should consider implementing an Incident Response Plan, which can be used in the event of a data security breach. An Incident Response Plan differs from a CISP in that it provides step-by-step instructions that the school district and its employees should follow if a data security breach occurs. Such a plan can be very helpful because in the moments following discovery of a breach, it can be difficult to identify who is in charge and what should be done.

The Incident Response Plan identifies the Breach Response Team and describes each team member's responsibilities. It appoints a single leader to be the final decision-maker. That person is sometimes the CPO, the Chief Information Security Officer, the head of IT, or the General Counsel. The Breach Response Team should include representatives from the following departments: superintendent's office, information technology department, law department, risk management, human resources (if employee data are involved), and the communications/public relations department. Other members can be added to fit the needs of a particular district or if the subject matter of a particular breach requires specialized expertise.

The Incident Response Plan should require that each employee bear responsibility for reporting suspected breaches to the Breach Response Team Leader. Once reported, the Breach Response Team Leader will triage the incident to determine if it is a "breach" that requires the Incident Response Plan to be deployed. The plan should

provide guidance to the Breach Response Team regarding conducting an investigation, communicating internally, mitigating any harm to systems or data, notifying affected individuals and/or regulators, and remedying the situation.

Once drafted, an Incident Response Plan should be tested to ensure its usefulness in the event of a security incident. This can be done by holding a mock breach exercise, and assessing how well the Breach Response Team worked through the mock breach using the Incident Response Plan. The U.S. Department of Education provides a Data Breach Response Training Kit for school districts.[28] This training kit provides instructions about how to hold a mock breach, what kinds of scenarios might work best, handouts, and other helpful guidance.

C. Acceptable Use Policy

Educational apps are often provided at low or no cost to educators who want to integrate technology into the classroom. Those apps require the educator to accept the terms and conditions of use, which can be a lengthy document written in "legalese." Acceptance of certain terms and conditions can expose an employee, the school, and the district to legal ramifications. In addition, students who have unfettered access to the internet may unknowingly expose themselves, their peers, the school, and the district to liability by accessing or using specific websites or educational apps. As a result, it is important to adopt and maintain a clearly worded Acceptable Use Policy governing all online activity, both internally and on the internet, for both staff and students. Consider incorporating school security policies into staff job descriptions, and assign specific individuals to monitor compliance. Computers housing sensitive data should be made physically inaccessible to unauthorized users, unnecessary services should be shut down, and staff should be trained to report lost or stolen equipment immediately. Students and employees should be required to sign an acknowledgement that they have received, read and understand the policy, and the penalties associated with failing to follow it.

D. Employee Training

In most school districts, protection of electronic data has been delegated to technology coordinators or other highly trained personnel, but staff training is now necessary for all employees to raise awareness of their legal obligations under applicable state and federal student and employee privacy laws, and to curtail inadvertent violations of students' and employees' privacy rights. Training should cover known or suspected risks, common errors that lead to breaches, district policies and the consequences of violating those policies. School districts should also require employees to sign a document indicating that they have received training and understand their responsibilities with respect to ensuring data privacy and security.

E. Monitoring of Data Security Capabilities and Procedures

As with any comprehensive approach to data managment, your data security capabilities should be monitored regularly, and procedures adjusted to reflect realities.

F. Cybersecurity Insurance

Though not a specific policy or procedure, school districts may want to consider the purchase of cybersecurity insurance, which may cover some of the costs associated with data security breaches. The insurance policy should be carefully reviewed by the district's attorney to ensure that the coverage provided meets the needs of the district, and that the district is aware of the coverage requirements.

5 What must a school district do to notify its community in the event of a data breach?

All 50 states and the District of Columbia have data breach notification laws. They require entities to notify affected individuals in the event the entity suffers a data breach that compromises the security or confidentiality of personal information it maintains. *See* Appendix B. The first data breach notification law was passed in California in 2003. There are important differences among the state laws, and navigating the patchwork of state laws can be a difficult and confusing process. You should work closely with your attorney as you develop procedures for notifying affected individuals in the event of a breach.

Though there is a general definition of the term "personal information" in California's initial law, some states have gone beyond that definition to include certain data points. In most states, "personal information" means a person's first name or first initial, and last name, in combination with a Social Security number, driver's license number, or financial account number and passcode or PIN to access that account. States have begun to expand

on that definition. For example, California's definition of "personal information" now includes medical or health care information. Other states have added precise geolocation and email addresses to the definition.

Most states require notification in the event of a breach of security, but the definition of what qualifies as a breach differs from state to state. In some states, a security incident is not a "breach" if there is no risk of harm to affected individuals. These states would allow a school district to conduct a risk of harm analysis prior to sending notification. If there is no identified risk of harm to affected students or staff, notification is not required. Other states do not allow such an analysis. For example, notification must be made in Illinois for a "technical" breach even if there is little to no risk of harm to affected individuals.

Some states impose a time limit for notifying affected individuals. Most states require notification "in the most expedient time available" and/or "without unreasonable delay." Some states now require notification to be made within 30 or 45 days of discovery. Most states also allow notification to be delayed at the request of law enforcement.

In addition to notifying affected individuals, some states require the breached entity to notify the state attorney general. Some states also require notification to go to the consumer reporting agencies if a large number of consumers, usually around 1,000 or more, have to be notified.

One federal law may have notification implications for school districts. The Health Insurance Portability and Accountability Act (HIPAA) regulations require notification by "covered entities" of data security breaches that impact "protected health information," as defined in the law.[29] In most cases, HIPAA will not apply to school district data breaches, even if they involve student or employee health information. Nevertheless, a school district must understand its obligations under HIPAA, including whether notification is required. If your school district has a contract with the state to assist in the provision of medical services to students, HIPAA will be implicated. Consult your school attorney to determine the extent of any HIPAA obligations your district may have.

The purpose of notification is to provide the affected individual an opportunity to take certain steps to protect himself from identity theft and other fraud. Some states require that data breach notification letters include specific content, including how the individual can notify the Federal Trade Commission or the state attorney general to obtain more information about identity theft. Breach notification letters usually include reminders to the victim of the breach

to check his or her bank statements and/or credit reports and to notify the credit reporting agencies or the bank in the event something does not look right.

6 What remedial services must a district offer to data breach victims? What other services should districts consider offering to affected individuals?

Individuals who receive notification letters have come to expect that the entity sending the letter will offer some kind of credit monitoring or identity theft protection free of charge, but in most states such services are not mandated. Only a few states require entities to provide credit monitoring under certain circumstances.

State law will likely control whether a school district may use public money in its regular operating budget to pay for remedial measures like credit monitoring or identity theft protection. School districts may be prohibited from using general funds to pay for such mitigating measures, particularly if the victim is not a student or school employee. In addition, cybersecurity insurance policies may help to cover the costs of remedial measures following a breach.

Credit monitoring and identity theft protection services are effective mitigating measures if the breached data includes individuals' Social Security numbers. Credit monitoring protects those individuals from having new credit accounts being opened using their names and Social Security numbers. If other data has been accessed, credit monitoring may not be as effective. For example, if a breach involves names and email addresses, credit monitoring will provide little benefit because the compromised data would not be sufficient to open unauthorized accounts. Credit monitoring can also be difficult to provide for children under the age of 18 who have no credit. If students are affected by a breach, take care to discuss options with credit reporting agencies to best protect those children from having credit established by an unauthorized individual.

After the Olympia School District in Olympia, Washington, was the target of a phishing scheme, school district officials consulted security experts, legal counsel, their insurance carrier, and their technology team in an attempt to explore all avenues towards securing employee personal data. Within two days, the district offered potential solutions to the breach. They suggested all employees independently apply for a free credit check and file an Identity Theft Affidavit Form with the IRS.

One message sent out by the OSD Communications Office suggested those affected by the scam remove birthdays from Facebook and other social media because tax returns cannot be fraudulently filed without them. Dates of birth were not included in the email received by scammers. As a result of the incident, the district planned to incorporate "additional safety and security training for all staff, especially as it relates to the transmission of private information via email, Internet, and phone".[30]

7 What should a school district do in the event of a data breach?

A. Hypothetical #1: The Lost Laptop

On Monday morning, a school administrator reports that her car was broken into over the weekend. Several items were stolen from her car, including a laptop that contained student data. (The administrator had taken the laptop home to do some work over the weekend.) The laptop was password-protected, but the data was not encrypted. The administrator called the police, who took a police report of the crime. The district has an Incident Response Plan. What's next?

Per the IRP, the incident must be reported to the Breach Response Team Leader ("Team Leader"). The Team Leader should direct the administrator to work with the IT department to identify all information on the laptop that was stolen. Early in the breach response process, the Team Leader should consult the district's school attorney to assess whether outside counsel should be consulted, and to determine if the district should file its own police report or otherwise get law enforcement involved. The Team Leader should notify the superintendent and the

entire school board, so that they can be prepared to respond to inquiries from the press, parents, students, and staff.

Once the Breach Response Team Leader has the report from IT regarding the information that may have been on the laptop, he or she can work with the district's school attorney to determine if breach notification is required under state or federal law, and whether to offer credit monitoring or identity theft services to affected students. The Team Leader also should work with other members of the Breach Response Team to develop any communications to students, parents, employees, the community, and the press about the incident.

Depending on the size of the incident, the Breach Response Team may want to use a call center to address student and parent questions and concerns. If that is the case, the Breach Response Team should then set up the call center parameters and develop a script for call center representatives. Once the message is finalized, the designated school district staff member can make the required notifications.

After notification is made, the school board and school district staff will likely receive press inquiries or other calls. In order to maintain a consistent message and not provide inaccurate or incomplete information, all calls should be routed through the call center, or through the Breach Response Team Leader, who may designate a communications lead.

Following the breach, district leadership should examine existing policies, especially those related to encryption of student data, and administrators' use of portable devices like laptops. If no such policies exist, the district should consider creating them. If a policy exists and it was violated, the district should consider disciplining the administrator for violating the district policy. The district should complete a final report on the steps taken to investigate, contain, and remediate the breach. The district should also review the breach response process against the Incident Response Plan to determine if any changes should be made to the Incident Response Plan.

B. Hypothetical #2: The Phishing Email

On Thursday evening, the school district's IT department receives a call from an administrator who says she may have responded to a phishing email. The administrator reports that the email looked like it came from the district superintendent and asked the administrator to click on a link to verify her email address. She clicked the link and provided her log-in credentials when requested. About a week later, she remembered the data security training she had taken that described phishing emails, and called IT. Though the school district trained its employees about phishing emails, it does not have an Incident Response Plan and has not designated a Chief Privacy Officer or Breach Response Team Leader. What's next?

Someone must be designated to lead the investigation and response. This can be difficult in the moments after

discovering a potential breach. Given the nature of the breach, someone from IT probably should lead the charge. The IT lead will then direct IT to investigate whether the system has been accessed by anyone without authorization using the administrator's credentials, and, if so, whether any data have been accessed. Once it is confirmed that the email did not come from the superintendent and was a phishing email, the system has been breached, and data accessed, the IT lead should work with the school district's legal department to determine whether law enforcement should be notified. It may also be appropriate to hire a third party forensic examiner, depending on the sophistication of the district's IT department.

The IT lead should also consult with the district's attorney about whether notification to affected district employees is required. Credit monitoring may be appropriate. The IT lead should call on someone in communications to develop a consistent message about the incident and determine whether a call center is necessary. Once these items are decided, the school district can make notifications pursuant to state or federal law and continue to respond to press and other inquiries with the agreed-upon message.

Following the breach, the district should determine if further training is necessary for employees on phishing emails and other security threats. The district should review its breach response process and consider codifying the process into an Incident Response Plan.

8 Where do I go for more information on data security for schools?

In addition to the *Forum Guide* and ED resources described above, your school district's IT staff may have access to resources with specific operational recommendations from organizations like the Consortium for School Networking. As student data privacy and security rules and norms continue to evolve, NSBA and its member state school boards associations will update resources that will be useful to you. Please regularly check www.nsba.org and your state school boards association website. If your school attorney is a member of NSBA's Council of School Attorneys, he or she will have access to updates and resources on the quickly evolving legal standards.

Appendix A – Data Breach Notification in Alabama

In 2018, Alabama became the last state in the union to pass a data breach law, but what does it mean for local boards of education? We hope these FAQs will answer your questions.

FREQUENTLY ASKED QUESTIONS

Where can I find the Data Breach Act?

The Act is codified in the Commercial Law and Consumer Protection Title at Ala. Code §8-38-1, et seq. and can be found here.

Who's covered by the Act?

Any entity that maintains sensitive personally identifying information ("SPII") is subject to the Act including individuals, nonprofits, corporations and governmental entities, including boards of education. Federal entities that operate under federal law are not covered. Third party agents, e.g. IT providers or IT security companies, who are hired to maintain SPII are also covered by the Act.

Who's protected by the Act?

Only Alabama residents.

What does the Act require?

The Act has three primary requirements for a covered entity. It must:

(1) Secure sensitive personally identifying information ("SPII");

(2) If a breach occurs, investigate the breach; and

(3) If a breach occurs, notify those impacted by the breach.

If the entity fails to provide proper notice, it can be subject to civil penalties by the Alabama Attorney General.

What data is protected?

SPII is defined as a person's name (full name or first initial and last name) if it's combined with one of these items:

- SSN or tax ID number;
- Driver's license number or other identifying number issued by the government;
- Bank account, credit card or debit card number if combined with a PIN, security code, password or expiration date;
- Medical information;
- Health insurance policy number or identification number; or
- User name/email address if combined with password or security questions and answers.

What data is not protected?

Information that is disclosed by the government pursuant to a public records request, or by widely distributed media is not covered.

What does the law require of boards before a breach occurs?

The Act requires that covered entities and third-party agents maintain reasonable security measures to protect SPII from a breach. Entities must consider all of the following:

- Designating an employee to coordinate security;
- Identifying internal and external risks;
- Adopting safeguards to address those risks and assess the effectiveness of those safeguards;
- Evaluating and adjusting security measures to account for changes in circumstances; and
- Keeping management, including the board of education and/or BOD, informed of the entity's security status. Boards of education can receive this information in executive session.

The reasonableness of an entity's security can consider the entity's size, the amount of SPII on hand and the cost of implementing security measures.

What does the law require of boards after a breach?

If a breach is discovered, the entity must investigate the breach and notify those impacted.
The investigation must include the following:

- An assessment of the nature and scope of the breach;
- An identification of any SPII involved and what people have been impacted;
- A determination of whether a wrongdoer has actually acquired SPII; and
- Implementation of measures to restore security following the breach.

Written notice to those impacted by the breach must be given as soon as possible, but must be done within 45 days of the discovery. That notice must be delivered by mail or email and contain:

- The date, estimated date or date range of the breach;
- A description of the SPII acquired;
- A general description of what the entity has done to restore security;
- A general description of what the individual can do to protect themselves from identity theft; and
- Contact information for the person they can contact about the breach.

Are there any exceptions to the notice requirement?

Yes. There are two exceptions to the above notice requirements:
First, if the notice is not feasible because of:

- excessive cost (given the resources of the entity or if the notice cost would exceed $500,000),
- lack of contact information for the impacted individuals, or
- if more than 100,000 people are impacted,

substitute notice can be provided by posting on the entity's website for 30 days, in print and broadcast media where the impacted people live, or in an alternative way with the approval from the Attorney General.
Second, if that notice would harm a law enforcement investigation, the notice can be delayed.

If the entity determines that notice should not be provided, it must document that determination and keep supporting records for 5 years.

Are there any other notice requirements?

Yes. If more than 1,000 people are impacted by the breach, the entity must notify the Attorney General in writing within 45 days. That notice must contain the following:

- a synopsis of the events surrounding the breach;
- the approximate number of Alabama citizens impacted;
- any free services being offered to impacted individuals, and instructions on how to use those services; and
- contact info for the person who can answer questions about the breach.

Additionally, if more than 1,000 people are impacted by the breach, the entity must notify all consumer reporting agencies.

What if a third-party agent is breached?

If a third-party agent is breached, it must notify the covered entity of the breach within 10 days of its discovery. The entity must then comply with the usual notice requirements. The entity may contract with the third party to provide required notices.

What are the penalties for failing to comply with the law?

If a nongovernmental entity fails to provide proper notice of a breach, the Attorney General is the only entity that can pursue a civil penalty under the Alabama Deceptive Trade Practices Act of up to $500,000 per breach. The failure is not a criminal offense and no individual can sue the entity for violating the Act.

What kind of penalty can school boards face?

Governmental entities are required to provide notice, but they are exempt from civil penalties. The Attorney General can, however, sue the entity to compel performance under the Act.

Appendix B – State Data Security Breach Notification Laws

Alabama	Ala. Code §§ 8-38-1 to -12	**Montana**	Mont. Code Ann. § 30-14-1704
Alaska	Alaska Stat. § 45.48.010	**Nebraska**	Neb. Rev. Stat. §§ 87-802 to -807
Arizona	Ariz. Rev. Stat. Ann. § 18-552	**Nevada**	Nev. Rev. Stat. § 603A.220
Arkansas	Ark. Code Ann. §§ 4-110-103 to 108	**New Hampshire**	N.H. Rev. Stat. Ann. §§ 359-C:19 to :21
California	Cal. Civ. Code § 1798.82	**New Jersey**	N.J. Stat. Ann. §§ 56:8-161 to -163
Colorado	Colo. Rev. Stat. §§ 6-1-713, -713.5, -716	**New Mexico**	N.M. Stat. Ann. §§ 57-12C-1 to -12
Connecticut	Conn. Gen. Stat. § 36a-701b	**New York**	N.Y. Gen. Bus. §§ 899-aa, 899-bb
Delaware	Del. Code Ann. tit. 6, §§ 12B-101 to -104	**North Carolina**	N.C. Gen. Stat. §§ 75-65, 75-61(10), 14-113.20(b)
District of Columbia	D.C. Code §§ 28-3851 to -3853	**North Dakota**	N.D. Cent. Code §§ 51-30-01 et seq.
Florida	Fla. Stat. § 501.171	**Ohio**	Ohio Rev. Code Ann. § 1349.19
Georgia	Ga. Code Ann. §§ 10-1-911 to -912	**Oklahoma**	Okla. Stat. tit. 74, § 3113.1
Hawaii	Haw. Rev. Stat. §§ 487N-1 to -4	**Oregon**	Or. Rev. Stat. §§ 646A.600 to .626
Idaho	Idaho Code Ann. §§ 28-51-104 to -105	**Pennsylvania**	73 Pa. Cons. Stat. Ann. §§ 2301-2308, 2329
Illinois	815 Ill. Comp. Stat. 530/5, 530/10, 530/15, 530/20, 530/45, 530/50	**Puerto Rico**	P.R. Laws Ann. tit. 10, §§ 4051-55
Indiana	Ind. Code §§ 24-4.9-1 to 24-4.9-5	**Rhode Island**	R.I. Gen. Laws §§ 11-49.3-1 to -6
Iowa	Iowa Code §§ 715c.1-2	**South Carolina**	S.C. CODE ANN. § 39-1-90
Kansas	Kan. Stat. Ann. §§ 50-7a01, 50-70a02	**South Dakota**	S.D. Codified Laws §§ 22-40-20 to -26
Kentucky	Ky. Rev. Stat. Ann. § 365.732	**Tennessee**	Tenn. Code Ann. § 47-18-2107
Louisiana	La. Rev. Stat. Ann. §§ 51:3071 to 51:3077	**Texas**	Tex. Bus. & Com. Code Ann. § 521.053
Maine	Me. Rev. Stat. tit. 10, §§ 1346 to 1350	**Utah**	Utah Code Ann. §§ 13-44-101, 13-44-201, 13-44-202, 13-44-301
Maryland	Md. Code Ann., Com. Law §§ 14-3501 to -3508	**Vermont**	Vt. Stat. Ann. tit. 9, §§ 2430, 2433, 2435, 2446, 2447
Massachusetts	Mass. Gen. Laws ch. 93H, §§ 1-6	**Virgin Islands**	V.I. Code Ann. tit. 14, § 2208
Michigan	Mich. Comp. Laws § 445.72	**Virginia**	Va. Code Ann. §§ 18.2-186.6, 32.1-127.1:05
Minnesota	Minn. Stat. § 325E.61	**Washington**	Wash. Rev. Code §§ 19.255.010 to 19.255.020, 42.56.590
Mississippi	Miss. Code Ann. § 75-24-29	**West Virginia**	W. Va. Code §§ 46A-2A-101 to -105
Missouri	Mo. Rev. Stat. § 407.1500	**Wisconsin**	Wis. Stat. § 134.98
		Wyoming	Wyo. Stat. Ann. §§ 40-12-501, 40-12-502

Endnotes

[1] FERPA is the federal law that protects the privacy of student records. 20 U.S.C. § 1232g; 34 C.F.R. Pt. 99.

[2] Natasha Singer, *Privacy Pitfalls as Education Apps Spread Haphazardly*, N.Y. Times at B1 (Mar. 12, 2015), available at http://www.nytimes.com/2015/03/12/technology/learning-apps-outstrip-school-oversight-and-student-privacy-is-among-the-risks.html.

[3] Nat'l Sch. Bds. Ass'n., Data in the Cloud: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era (April 2014), https://www.nsba.org/-/media/NSBA/File/legal-data-in-the-cloud-guide.pdf?la=en&hash=D74E3D55A0ED0073AE530A079F83F9280CF4BD25.

[4] See, e.g., Information Protection @MIT, https://infoprotect.mit.edu/risks-to-data https://ist.mit.edu/security/data_risks (last visited Aug. 26, 2019).

[5] Privacy Rights Clearinghouse, *Data Breaches*, https://www.privacyrights.org/data-breaches.

[6] Kristen Taketa, *San Diego Unified data breach hits staff, plus as many as 500,000 students,* Los Angeles Times (Dec. 31, 2018), https://www.latimes.com/local/lanow/la-me-ln-san-diego-unified-data-breach-20181221-story.html.

[7] Privacy Rights Clearinghouse, *Central Islip Union Free School District: Security Breach Letter* (Feb. 13, 2018), available at https://www.privacyrights.org/data-breaches.

[8] Ponemon Institute LLC, IBM, *2019 Cost of Data Breach Report* at https://www.ibm.com/downloads/cas/ZBZLY7KL.

[9] Nat'l Forum on Educ. Statistics, U.S. Dep't of Educ., Forum Guide to Education Data Privacy, NFES 2016-096 (July 2016), https://nces.ed.gov/pubs2016/NFES2016096.pdf.

[10] *Id.* at *11.

[11] U.S. Dep't of Educ., Data-Sharing Tool Kit for Communities: How to Leverage Community Relationships While Protecting Student Privacy (Mar. 2016), https://www2.ed.gov/programs/promiseneighborhoods/datasharingtool.pdf.

[12] *Id.* at *14.

[13] U.S. Dep't of Educ., Data Security Checklist (Rev. July 2015), https://studentprivacy.ed.gov/resources/data-security-checklist.

[14] U.S. Dep't of Educ., Best Practices for Data Destruction (Rev. March 2019), https://studentprivacy.ed.gov/resources/best-practices-data-destruction

[15] U.S. Dep't of Educ., Data Breach, https://studentprivacy.ed.gov/topic/data-breach.

[16] 201 CMR 17.03(1).

[17] *Id.*

[18] *See* Data Security Checklist *supra* note 15 and resources available at http://studentprivacy.ed.gov/topic/security-best-practices.

[19] *See supra* note 15, Data Security Checklist.

[20] *Id.*

[21] 20 U.S.C. § 1417(c).

[22] 34 C.F.R. §§ 300.624(b), 303.416(b) (IDEA regulations allow a permanent record of the child's name, date of birth, parent contact information, and other select data to be maintained without time limitation.).

[23] Center for Digital Education, *Issue Brief — Safeguarding Student Data in the Age of Digital Learning: Responsible privacy practices for K-12 school districts* (2016), https://ess.csa.canon.com/rs/206-CLL-191/images/K-12-Issue-Brief-Safeguarding-Student-Data.pdf.

[24] N.Y. Educ. Law § 2-d(2).

[25] *Id.*

[26] *Id.* § 2-d(2)(b).

[27] *Id.* § 2-d(2)(c).

[28] *See* https://studentprivacy.ed.gov/resources/data-breach-response-training-kit.

[29] 45 C.F.R. §§ 164.400-.414.

[30] Greg Mohan, *Data Breach at Olympia School District: Employees (sic) personal information released in phishing scam,* The Cooper Point Journal, May 4, 2016, https://www.cooperpointjournal.com/2016/05/04/data-breach-at-olympia-school-district-employees-personal-information-released-in-phishing-scam/.

ALABAMA
ASSOCIATION OF
SCHOOL BOARDS

nsba
National School Boards Association

1680 Duke Street, FL2, Alexandria, VA 22314
www.nsba.org