TESTIMONY OF THE

PENNSYLVANIA SCHOOL BOARDS ASSOCIATION

BEFORE THE HOUSE EDUCATION COMMITTEE

REGARDING

STUDENT DATA PRIVACY AND PROTECTION

ELISHA POSPISIL

FOREST AREA SCHOOL DISTRICT, DIRECTOR OF CURRICULUM AND TECHNOLOGY

Chairman Sonney, Chairman Longetti, and members of the House Education Committee, thank you for inviting the Pennsylvania School Boards Association (PSBA) to testify today on behalf of the 5,000 local public school leaders they represent. My name is Elisha Pospisil and I am the Director of Curriculum and Technology for the Forest Area School District. I come to you with over 20 years of experience in public education that includes time spent as a teacher, an instructional technology coach, a building principal, and a District administrator. Unlike many Tech Directors, my background is in education rather than IT and I hope that this perspective will be helpful to you as you consider the future of student data privacy in Pennsylvania. I appreciate the opportunity to present testimony about the issues surrounding student data privacy and retention that are currently facing our schools. The ever-rising risk of phishing attacks, ransomware, and identity theft, along with our increased reliance on cloud-based software and data storage, have made the importance of student information security more urgent than ever before.

Records Retention

In the Forest Area School District we retain student records throughout a student's time in our District and as required after they have graduated or withdrawn. These records include academic, school counseling, special education, discipline, and medical files. The records are retained in accordance with state guidelines and the District Student Records Procedure. Per these guidelines, medical records and student portfolios are purged or returned to students at withdrawal or graduation. Discipline, attendance records, and school counseling files are destroyed 6 years after a student graduates or withdraws. State assessments and student transcripts are kept on file as prescribed by school code and district policy.

The District does not specifically collect or retain parent/legal guardian data. Any parent information that is collected is specific to the student. Some data, such as address and phone number, pertaining to guardians may be included in enrollment records or emergency contact information. Some of this data may also be included in court orders or custody agreements that are part of a student's file while they are in school.

Record Storage and Security

When it comes to student data, we currently use many services that require electronic data input and backups. Our current student information system, special education management software, email, and transportation systems are all in the cloud. Additionally, we are using many web-based software programs to provide students with practice of academic skills and to assess their progress. All of these systems collect student data to varying degrees. While these cloud-based systems are useful and necessary in many ways, they also limit our control over the retention and security of the data stored within them.

Local electronic data storage is also a reality that demands our attention. When files have expired they are deleted and backups of those files are discontinued. When hardware is disposed of, hard drives are wiped or destroyed. In addition to electronic student data we also maintain some traditional paper files. These files are kept in a locked room with limited access and either returned to students or shredded at the appropriate time according to policy.

Safety Precautions

In our efforts to protect student information and privacy we use a firewall to limit traffic in and out of our local network and we use Internet filtering to limit student Internet access per the Children's Internet Protection Act (CIPA). The Family Educational Rights and Privacy Act (FERPA) provides direction about what student information schools can share with outside agencies. Internally, we have developed a student records retention schedule, deployed a backup system for locally stored electronic records, added cybersecurity to our insurance policy, and followed industry recommendations for anti-virus, password conventions and multi-factor authentication. Multiple WiFi networks are used to separate devices that need access to local data systems and those that do not. We review user terms and conditions for all vendors before we sign any contracts or agreements and we limit vendor access to our internal systems. In addition, and perhaps most importantly, we have been providing short intermittent cybersecurity training for all District employees. These trainings serve as regular reminders to staff and encourage good habits that will help adults in our District recognize phishing attempts that might lead to the disclosure of student or employee information that could be detrimental to the individual or the District. Students learn about the importance of guarding their online data as part of the curriculum.

The Forest Area School District has adopted policies and procedures to ensure proper management and disposal of student records. These policies and procedures include guidelines for student records management and retention and acceptable use of Internet, computers and network resources. We have developed a Continuity of Operations IT Plan to guide our decisions and we also have a policy that outlines steps to be taken in the case that personal information of students or employees is breached.

While we have gone to great lengths to ensure the safety of student data we still face some challenges. Like many districts in our area, we have a very small IT staff. Our time for reading user agreements, keeping up to date with cybersecurity recommendations, and acting on those recommendations is sometimes limited by our need to address immediate issues that directly impact instruction and learning. Guidance on what the expectations are for cybersecurity in K-12 schools has been varied and sometimes inconsistent and while vendor agreements outline expectations for both parties, beyond the agreement, we have very little access to vendor records that indicate the use or destruction of student data after its collection. Those agreements are often written in legalese which can make them challenging and expensive to interpret as our district does not have a legal department and any contract reviews must be outsourced to our solicitor. When it comes to network monitoring and penetration testing, private services can be costly and require in-depth vetting.

Keeping Up to Date

Typically, in the Forest Area School District, we look to recommendations from the Cybersecurity & Infrastructure Security Agency (CISA) and the Department of Homeland Security (DHS) for guidance about cybersecurity and issues related to student privacy, records retention, and data protection. While the resources provided by these agencies are very thorough and well done, we have found that they are often scaled beyond what is necessary for

our small district and we are still left looking for answers that are appropriate for our specific circumstances.

Recommendations

Based on my experiences in public education as they relate to student data and security, I would like to make the following recommendations:

The state can assist schools in terms of data protection, retention, and safety by:

a. Designating parameters that limit the types of student data that can be collected by vendors, what that data can be used for, and how long it can be retained;
b. Providing clear guidance to schools about electronic student data and best practices in regard to the retention and destruction of data;
c. Creating a clearinghouse of vendors that have already been screened and meet specifications for student data use and privacy;
d. Providing state resources to school districts and supporting the use E-Rate funding for cybersecurity; and
e. Encouraging cybersecurity vendors to participate in state-wide cooperative purchasing programs such as PEPPM and CoSTARS

Conclusion

In conclusion, school districts throughout the Commonwealth are working diligently to protect student data and ensure that records are both retained and disposed of in responsible and ethical ways. Any support that the legislature can provide in terms of guidance for K-12 cybersecurity, limitations or guidelines for vendors, or vetting of and access to cybersecurity vendors will be greatly appreciated. I thank you for the opportunity to speak today and I will be happy to answer any questions you may have.

Attachments:

Enrollment Checklist
216 Student Records
    Forest Area Student Records Procedure
    Forest Area Records Management Plan Appendix A - Litigation Hold
800 Records Management
    800 - AR Records Management
830 - Breach of Computerized Personal Information
815 - Acceptable Use of Internet, Computers and Network Resources
Forest Area Continuity of Operations IT Plan