THE WINNETKA
PUBLIC SCHOOLS
DISTRICT 36

A Community of Learners

Informational Memo - Data Security and Privacy

TO: School Board
Superintendent Dr. Trisha Kocanda

FROM: Maureen Miller, *Director of Technology*

February 25, 2020

Overview & Background

Data privacy and security are integral to the operation of any school district. Through the years the threat landscape has evolved as data breaches have become more frequent and schools, who were not often targets in the past, are being seen as more vulnerable to breaches and threats. The school district endeavors to maintain the confidentiality, integrity, and accessibility of student data, while still allowing students to obtain a technologically rich educational experience.

The federal student privacy laws that regulate privacy and protect sensitive data when schools issue devices or use educational software are best known as FERPA and COPPA. FERPA, or the *Family Educational Rights and Privacy Act*, protects the privacy of student education records. *The Children's Online Privacy Protection Act* (COPPA) addresses the protection of data for children under the age of 13. Both laws focus on the ongoing and ever-evolving challenge of protecting student data privacy.

Beyond Federal Laws, schools must comply with state and local ordinances. Recently, Illinois legislation was passed to update the *Student Online Personal Protection Act (*SOPPA). The new Illinois law requires much more transparency from school districts.

Student data is not the only data that a school district must protect. Financial data is also at risk for the school district and district employees. Systems must be in place to secure and protect all forms of data. This includes management of logins and granular control of systems to ensure everyone who needs access to student and staff information have access, but not more access than their role requires.

In the past, the responsibility of data security has fallen to the technology department. With the increase of technology systems and software being implemented across all departments, these departments now play a key role in protecting student and staff data.

The Winnetka Public Schools has partnered with CoSN, Consortium of School Networking, an international organization that has developed a "Trusted Learning Environment" seal for school systems focused on building a culture of trust and transparency around data privacy. (More on TLE: refer to April 2019 memo)

The TLE program requires school systems to have implemented high standards for student data privacy protections around five core practice areas: Leadership, Business, Data Security, Professional Development and Classroom. School systems that meet the Program requirements will earn the TLE Seal, signifying their commitment to student data privacy for their community.

In preparation for applying for the TLE seal, the Director of Technology has been working with other area technology directors to understand the privacy landscape and legal obligations, to conduct a comprehensive technology audit, to establish a data governance plan, and to establish data protection training for staff. This work has included workshops with data security and privacy experts, quarterly meetings with a CoSN Trusted Learning Environment mentor, and weekly progress checks with participating school districts to share resources related to earning the TLE seal.

Project Timeline to Date

Date	**Action**
December 2018	Partnered with KnowB4 to provide security awareness training for all staff. KnowB4 provides phishing training and hoax templates, allowing the District tech team to target those individuals who are prone to click on a hoax email.
April 2019	Conducted an Infrastructure Assessment with ClientFirst Consultants. Their team determined areas of strengths and key areas for improvement. Since the audit, the team has improved documentation, started cross-training, and developed a disaster recovery plan.
Ongoing	Trusted Learning Environment Seal components- see TLE work here

February 2020	Partnered with Wilmette School District 39, Kenilworth School District 38, New Trier Township School District 203, and Halock Securities to review data policies and practices currently in place and identify opportunities for addressing vulnerabilities. This review will take place through the Spring and Summer, beginning with security interviews in March of 2020.

Next Steps

- Designate the Director of Technology as a staff privacy officer to carry out the duties required to maintain compliance with data security procedures.
- Create a website dedicated to data privacy and transparency that includes a public list of all third-party vendors that handle student personally identifiable information (PII)
- Continue work towards the CoSN TLE Seal with an anticipated application date to be October of 2020
- Conduct regular audits to determine which online technologies are in-use
- Continue to review and update School Board policies to comply with evolving legal and best practice changes

Additional information on federal and state laws:

- FTC COPPA FAQ
- USDOE FERPA FAQ
- SOPPA (Illinois)