

MN Student Data Privacy Bill

AMSD Meeting May 6, 2022





History

- Some version of this bill has been around for the last 6 years
- Earlier versions were more restrictive with Opt-in language
- House and Senate versions were very different
- The originality of this bill has been an interest convergence between groups
 - Minnesota Advocates and Champions for Children
 - Minnesota ACLU
- The key topics with this bill have been around:
 - Unwarranted surveillance
 - Privacy of student information
 - Parents right to direct education



Our key interests

- Teachers are able to effectively use digital tools that enriches, enhances, and produces high quality learning experiences for our scholars
- Districts are able maintain effective operations of schools
- District can meet meet the requirements of state and federal laws
- Districts can ensure cyber security
- Districts can ensure the safety of our scholars with district provided technology and technology systems



This legislative Session (House)

- The new bill version was first introduced in the house by Rep. Feist
 - HF341
- The original version had many significant issues
 - Opt-out language
 - Monitoring restricted unless there was a warrant or imminent threat to life and safety
- Several changes were made on the House version
 - The most significant change was in monitoring to allow for finding lost/ stolen equipment, meet state/ federal law, align with CIPA requirements for e-rate funding, and allowing for instructional use
 - Opt-out still remains



This legislative Session (Senate)

- Senate version that mirrored the house version was introduced by Sen. Bigham
 - SF2307
- Sen. Mathews was added as Chief Author
- Sen. Mathews, Rep. Feist, and Rep. Scott continued to review our concerns
- New language was amended on May 4th that addressed our concerns
 - Opt-out language has been completely removed



What you need to know

- The current version in the Senate puts majority of requirements on tech vendors to ensure privacy and security
- Districts have a responsibility to provide notice of what digital tools are used in their system that contain student data
- Districts have a requirement to notify within 72 hours if a students digital device/ information was accessed to “*respond to an imminent threat to life or safety*”