St. Cloud Area School District 742 – (DRAFT 2) Resolution 2025-3
Establish Minnesota Privacy and Cybersecurity for Education (PACE) Council

2025 Delegate Assembly
Proposed Legislative Resolutions
RESOLUTION 2025-3 - Establish Minnesota Privacy and Cybersecurity for Education (PACE) Council
SUBMITTED BY: St. Cloud Area School District 742

Recommendation

St. Cloud Area School District 742 supports and recommends that the Minnesota School Boards Association (MSBA) advocate for the creation of a statewide council to develop a unified approach to updating and securing data privacy agreements with third-party vendors and to strengthening cybersecurity measures.

Background Information

Minnesota's public schools are rapidly adopting AI-enabled and cloud-based educational tools, even as data privacy obligations expand under laws such as the Minnesota Consumer Data Privacy Act (effective July 31, 2025). Many districts, particularly smaller and rural systems, lack the specialized legal, technical, and procurement capacity to evaluate vendor data practices or negotiate strong protections.

Building on Minnesota's proven cooperative models, this resolution proposes the creation of statewide **Privacy and Cybersecurity for Education (PACE) Council** to:

- Maintain standardized vendor assessments and model contract language (including AI transparency, data minimization, ownership rights, and verified deletion); and
- Issue unified privacy and cybersecurity guidance that districts
- Certify vendors who meet statewide privacy and cybersecurity standards and maintain this list publicly for districts to view

Participation would remain advisory and opt-in, preserving local board authority while lowering costs and improving protections for students, families, and staff.

Whereas Statements

WHEREAS, Minnesota's publicly funded schools face increasingly complex privacy compliance obligations alongside the rapid expansion of AI-enabled educational technologies; and

WHEREAS, individual districts - especially small and rural systems - often lack the specialized technical, legal, and procurement expertise required to evaluate vendor data practices and negotiate strong data-protection terms; and

WHEREAS, Minnesota school districts must comply with multiple overlapping laws—Family Educational Rights and Privacy Act (FERPA), the Minnesota Government Data Practices Act, (MNGDPA), Children's Online Privacy Protection Act (COPPA), and the Minnesota Consumer Data Privacy Act (effective July 31, 2025)—creating complexity best addressed via coordinated guidance and shared services; and

WHEREAS, existing frameworks such as Consortium of School Network (COSN's) essential skills for data management and cybersecurity, while foundational, are inadequate in an AI-enhanced environment because they don't tackle:

- **Algorithmic transparency and bias**—understanding how AI models make decisions, the training data behind them, and potential impacts on students;

- **Vendor due diligence for AI tools**, which are often opaque, evolving, and trained on sensitive data in ways traditional contracts did not anticipate;

- **Machine learning risk management**, including alignment with frameworks like the **National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF);**

- **Ethical and pedagogical assessment**, such as evaluating the efficacy of AI tools and knowing when not to deploy them;

- **Data lifecycle challenges in AI contexts**, where deletion verification in models ("machine unlearning") is far more complex than in standard databases; and

WHEREAS, current state cybersecurity efforts like MNIT's incident reporting and Cyber Navigator program address breaches—but not these AI-specific governance needs (transparency, bias, accessibility, AI data processing in contracts); and

WHEREAS, the Minnesota Consumer Data Privacy Act (MCDPA), effective July 2025, imposes new obligations on controllers and processors of personal data, further increasing the need for coordinated implementation support for districts and vendors; and

WHEREAS, Utah's State Board of Education has created a statewide Data Privacy Agreement (DPA) that aligns with FERPA and state privacy laws and serves as an "umbrella" or "piggy-backable" contract. Once a vendor signs it, any Local Education Agency (LEA) needing that vendor's services simply sign a one-page Exhibit E to join the agreement. This eliminates the need for repetitive negotiations, offers vendor transparency, assures compliance, and speeds procurement—effectively granting statewide access to vetted agreements; and

WHEREAS, a statewide council can replicate these efficiencies in Minnesota - providing model contract language, vendor assessments (including AI oversight), and shared guidance that preserves local governance and lowers costs; and

WHEREAS, this initiative is focused on protective infrastructure, not instructional content or curriculum, and is meant to strengthen local policy while layering in expertise; and

Now, Therefore, Be It Resolved that the Minnesota School Boards Association urges the Minnesota Legislature to establish **a Minnesota Privacy and Cybersecurity for Education (PACE) Council to**:

- Maintain standardized privacy requirements and model agreements for educational technology and Artificial Intelligence (AI) vendors, including efficacy disclosures, data minimization, ownership limits, and verifiable data deletion;

- Provide unified guidance, practical tools, and optional model policies to help districts navigate privacy and AI adoption responsibly; and
- Establish a **centralized, statewide DPA system** that is legally binding across all LEAs—mirroring Utah's model for efficiency, consistency, and stronger student-data protection;
- Strengthen school cybersecurity capacity—access to expertise, training, and shared response resources;
- Ensure accessibility compliance (IDEA/Section 504) in privacy and cybersecurity standards;
- Mandate integration of AI risk management, algorithmic transparency, bias mitigation, and pedagogical suitability—aligned to standards like NIST's AI RMF;
- Secure dedicated state funding and alignment with federal funding, with continuity even if federal support wanes.

BE IT FURTHER RESOLVED that the PACE Council's enabling language must include:

- **Scope**: Provide advisory central guidance without creating procurement bottlenecks;

- **Participation**: Vendor compliance must be required for contracts with Minnesota schools; district uptake of shared services remains voluntary and state-supported;

- **Membership**: Include school boards, district leaders, higher ed, MNIT, and privacy/cyber experts;

- **Facilitation**: Convene the council via a cross-sector collaborative, like the Minnesota Generative AI Alliance (MNGAIA) for Education;

- **Reporting**: Provide an annual legislative report covering activities, guidance, and recommendations.

Supporting Rationale

A coordinated, statewide approach drawing on expertise across sectors offers the most effective and efficient way to address the complexity of modern AI governance, privacy management, and cybersecurity readiness. While many districts lack access to specialized knowledge and resources, a statewide council can harness cooperation, reduce costs, and deliver timely, pragmatic solutions when they are most urgently needed.

This resolution is not only about compliance - it is about safeguarding students, families, and staff from harm. Strengthened privacy and cybersecurity protections reduce the risk of identity theft, cyberbullying, and commercial misuse of personal data. Clear standards and shared expertise also help ensure AI and digital tools used in classrooms are safe, accessible, and inclusive, supporting students of all abilities.

With current district protections heavily reliant on federally funded cybersecurity and Safe Schools grants, potentially resources that face uncertain renewal, the PACE Council provides Minnesota with a stable, state-level framework to sustain protections even if federal dollars diminish.

Equally critical, coordinated incident response capacity will allow school districts to prepare for, manage, and recover from data breaches or cyberattacks swiftly and effectively. By combining prevention with shared response resources, the PACE Council will ensure that Minnesota schools can protect sensitive data and restore operations with minimal disruption. Together, these measures will reinforce public trust that Minnesota schools take seriously their responsibility to create safe, secure, and equitable learning environments in the digital age.

Because no existing state division has the specialized expertise to lead this work, establishing a council of practitioners and experts, facilitated by MNGAIA, provides an essential interim structure until a permanent state capacity can be developed.