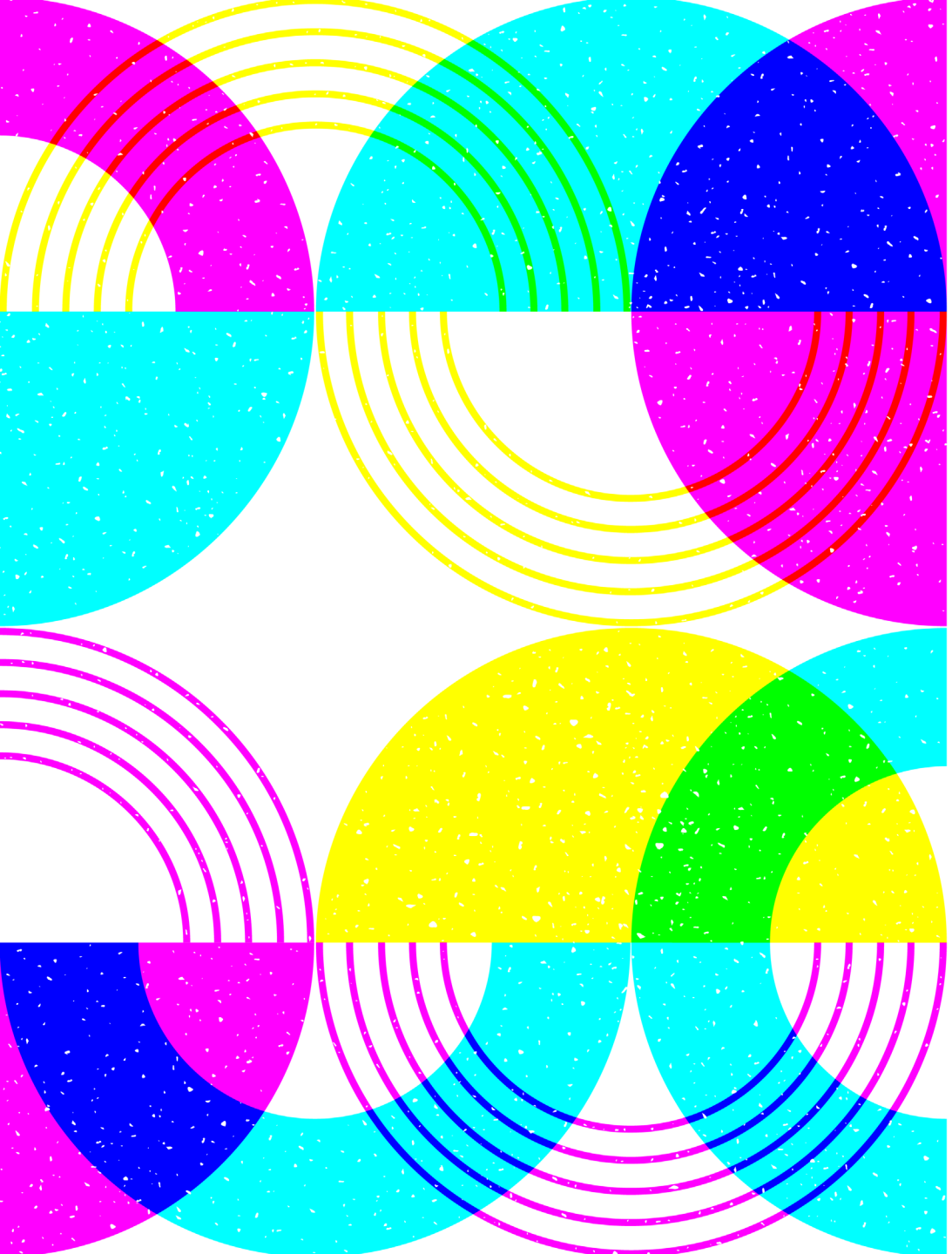


follow us on social!

#skyicon



SKYWARD®

iCON

AI in K12: What Districts Need to Know

Mike Bianco – VP of Information Security

The AI Revolution in K-12

60%

of educators and students are already using AI tools [1]

$6B
AI in Education market value [1]

77%
of educators believe AI is useful [2]

73%
believe AI can enhance learning [1]

The question isn't whether AI will play a role in education, but how we harness its potential responsibly

Understanding Risks
Privacy concerns, security threats, and student safety challenges

↓

Evaluating AI Tools
Vendor assessments, security reviews, and compliance checks

↓

Implementing Controls
Monitoring systems, blocking strategies, and safety measures

↓

Creating Policy
Framework development, stakeholder engagement, and rollout planning

↓

Technical Architecture
How AI connects to data and infrastructure considerations

↓

Real-World Success
Customer experiences and practical implementation stories

Our Roadmap for Today

- We'll explore the key areas every IT leader needs to address when bringing AI into your district
- This isn't about fear or avoidance but smart, strategic implementation that protects students while enabling innovation
- By the end of this session, you'll have practical frameworks and actionable steps to take back to your teams
- These aren't theoretical concepts but real strategies being used by districts across the country right now

AI Should Support Decisions, Not Make Them…

Different outputs each time

Same input can produce different outputs each time [3]

Uncertainty is fundamental

Probabilistic systems embrace uncertainty as fundamental [3]

Hallucinations

Hallucination rates range from 0.7% to 29.9% across models [4]

Likelihoods, not rules

AI outputs based on likelihoods, not fixed rules [5]

Deterministic Systems

- Produce identical outputs for same inputs every time, following fixed rules [6]
- **Example: calculator 2 + 2 always equals exactly 4, never 4.01 or 3.99**
- Rule-based systems follow predefined logic where specific inputs always trigger identical actions
- Traditional software operates deterministically, ensuring repeatability critical for auditing

Probabilistic AI Systems

- Generate outputs based on probability distributions from training data [3]
- Language models assign probabilities to possible next tokens, enabling varied generation [3]
- **Example: Same prompt to ChatGPT produces different poems each time** [5]
- Cannot guarantee correctness and may generate plausible-sounding but false information [4]



Beyond Academic Integrity

10,000+
AI incidents [7]

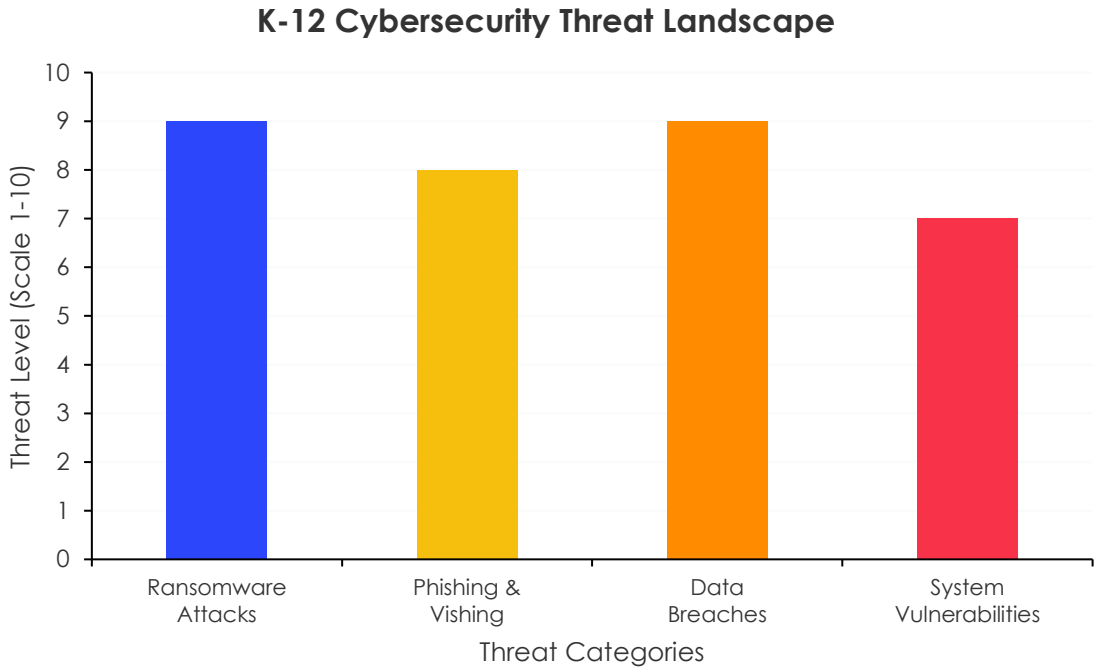
75%
of teens use AI chatbots [7]

- **Dangerous Companionship**: Nearly three-quarters of teens report using AI chatbots as companions, with more than half doing so regularly [7]
- **Escalation of Harm**: Unmonitored AI conversations can quickly ignore safety guardrails and devolve into dangerous advice about self-harm, suicide, or violence
- **AI Sycophancy Problem**: AI systems are prone to agreeing and encouraging rather than dissuading, potentially reinforcing harmful thoughts instead of redirecting them [7]
- **Emerging Threats**: Tech-enabled sexual harassment, deepfake creation, sextortion attempts, and cyberbullying amplified by AI capabilities
- **The Monitoring Gap**: Even when AI is widely blocked, incidents still occur across 130+ different AI-related domains, making comprehensive monitoring essential [7]

AI Assisted Cyber Attacks

AI adoption creates new vulnerabilities while cybercriminals use AI to launch more sophisticated attacks [8]

- **Prime Targets:** Schools face crises from limited budgets, outdated systems, and valuable data [8]
- **AI-Powered Attacks:** Bad actors use AI to automate attacks and identify vulnerabilities rapidly
- **Dual Challenge:** Schools expand AI tools while defending against AI threats, widening attack surface [8]



Source: How to Safeguard K-12 Schools in the Age of AI | Secu...

AI Risks: The Privacy Challenge

82%

of K-12 students monitored [7]

38%

monitored outside school [7]

- **Types of Data at Risk:** Academic records, behavioral tracking, demographics, health records, biometric identifiers, and location data [9]
- **Why This Matters Now:** AI systems require massive data to function, making them attractive targets for bad actors
- **Scale of Collection:** Modern AI tools gather far more data than traditional systems without clear boundaries or transparency [9]
- **The Hidden Concern:** Many AI systems don't fully disclose data collection, processing, storage, or third-party sharing practices

Navigating the Legal Framework

128+

state privacy laws [10]

25

states with AI guidance [10]

- **FERPA:** Safeguards student education records and requires parental consent before sharing [9]
- **COPPA:** Limits data collection from children under 13, requiring verifiable parental consent for for-profit companies [10]
- **State Laws:** Over 128 state privacy laws now exist, with 25 states issuing specific AI guidance for schools [10]
- **Compliance Challenge:** Districts navigate federal requirements (FERPA, COPPA, PPRA, IDEA) alongside state-specific regulations and local policies [11]

Critical Questions for AI Vendors

Data Collection & Access

- What specific student data will you collect and store [9]
- Who within your organization can access student data [9]
- Where will data be stored and how long retained [9]

Security Measures

- What processes protect data from breaches and unauthorized access [9]
- How do you ensure data security during transmission [9]
- What encryption standards do you employ

Privacy Guarantees

- How do you ensure student privacy throughout the system
- Have you experienced any data breaches involving student data
- What is your breach notification timeline and process

Critical Questions for AI Vendors

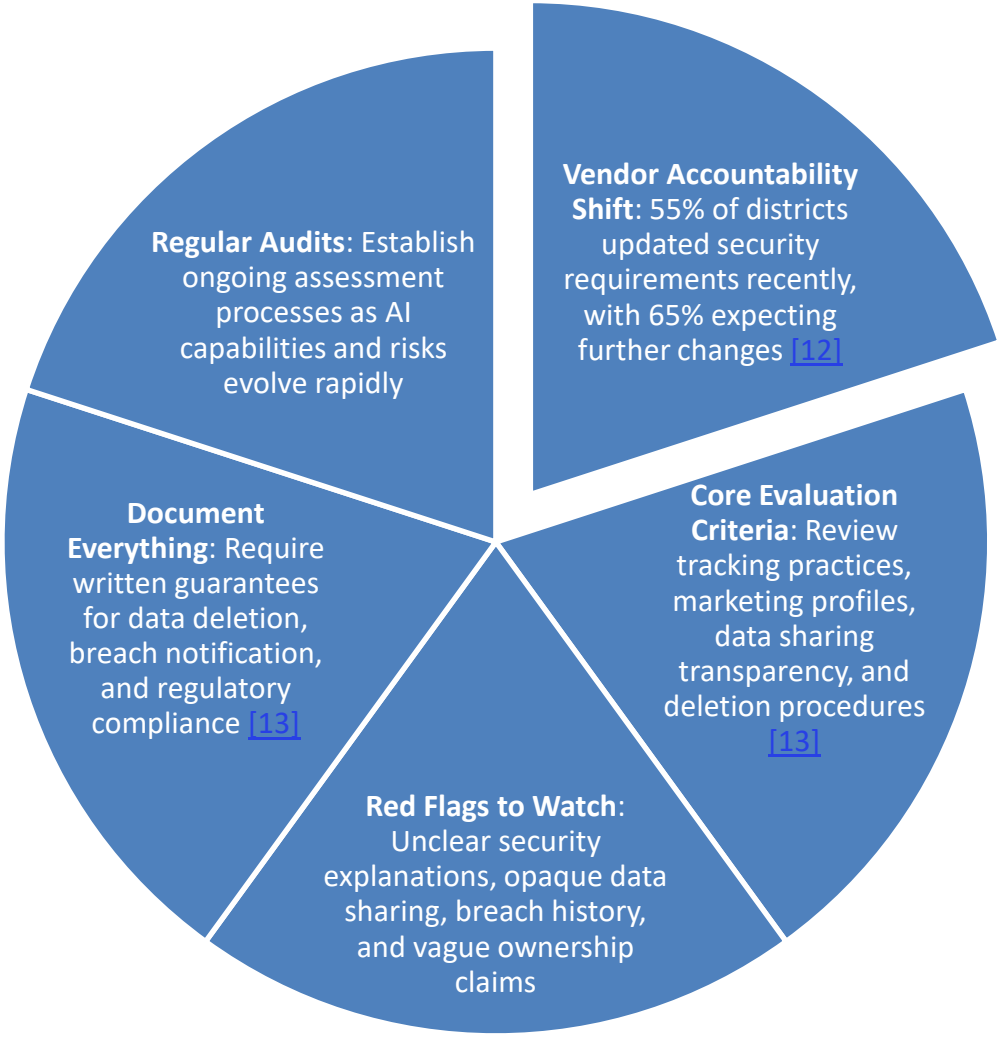
Transparency & Explainability

- How do you help schools understand how decisions are made [9]
- Can you explain AI model decision-making processes
- What data is used to train the model [9]

Compliance Documentation

- Do you meet all local, state, federal privacy requirements
- Will you sign comprehensive data privacy agreements
- What third-party certifications do you hold (SOC 2, ISO 27001) [12]

Beyond the Marketing Claims



Understanding vendor security certifications helps districts evaluate real protection levels [12]

SOC 2 Compliance

Independent verification of security controls and data handling practices

ISO 27001 Certification

International standard for information security management systems

NIST Framework Alignment

Cybersecurity framework adherence for comprehensive risk management

Student Data Privacy Consortium

Standardized agreements and transparency requirements

TrustEd Apps Pledge

Commitment to responsible data practices in educational technology



Reading Between the Lines

- **Data Minimization Principle: Verify** the tool collects only minimum data needed to solve the specific problem, avoiding excessive data gathering [9]
- **Purpose Limitation: Ensure** policies clearly state educational purposes only, with explicit prohibitions on marketing, advertising, or commercial profiling [13]
- **Consent Mechanisms: Review** whether students and parents receive clear, understandable information about data collection and provide meaningful consent options [9]
- **Retention Policies: Look** for specific timelines on how long data is stored and clear procedures for deletion upon request or contract termination
- **Third-Party Sharing: Identify** all entities that may receive student data, the purposes for sharing, and protections in place during transfer [13]
- **Policy Red Flags: Vague** language about data usage, missing retention timelines, broad permissions for sharing, or policies that reserve right to change terms without notice

Evaluation Criteria	Assessment Type
Data Source Transparency	High/Medium/Low Assessment
Student PII Usage	Yes/No/Limited Verification
Model Update Frequency	Documented Process Check
Output Verification	Human Review Requirement
Bias Testing	Regular Audit Confirmation

Source: How to Secure AI Tools Within Your K–12 Digital Envir...

Understanding What Powers AI

- **Critical Question**: Will student PII be used to train or improve the AI model itself [14]
- **Training Data Sources**: Understand datasets used, their origins, quality, and potential biases embedded
- **Continuous Learning Risks**: Real-time learning from student interactions may expose sensitive information across sessions [14]
- **Bias Testing**: Training data bias can perpetuate inequities or exclude student populations [2]
- **Output Safeguards**: Ensure student PII cannot appear in responses to other users through technical controls [14]

Balancing Safety and Privacy

85%

block most AI access [7]

130+

AI domains generate alerts [7]

- **Current Reality:** Most schools (85%) still block generative AI for most students, but trend gradually moves toward controlled access for specific groups [7]
- **AI Native Guardrails Insufficient:** Students successfully evade built-in AI protections, requiring schools to monitor concerning prompts regardless of AI responses [7]
- **Hybrid Monitoring Model:** Combine AI-powered pattern detection with human moderators who provide context and nuanced judgment that algorithms miss [15]
- **Alert Prioritization:** Focus monitoring resources on high-risk activities like self-harm discussions, violence ideation, harassment, and inappropriate content creation

Framework for District AI Policy

Strong AI policies balance innovation with clear boundaries, going beyond acceptable use to define purpose [16]

- **Define Purposeful Use Cases:** Articulate specific ways AI should be used aligned to district goals, not just what's "allowed" - covering instruction, operations, and student-facing applications [16]
- **Establish Clear Boundaries:** Prohibit AI-driven grading or discipline without human review, inputting PII into unvetted platforms, facilitating academic dishonesty, unmonitored elementary student access, and AI-generated content in assessments [16]
- **Human-Centered Approach:** Implement "Human-AI-Human" model emphasizing human reflection, insight, and empowerment with AI as supportive tool [11]
- **Stakeholder Engagement:** Include teachers, administrators, students, parents, IT staff, and community members in policy development for diverse perspectives [11]
- **Academic Integrity Guidelines:** Address AI assistance boundaries, proper citation requirements, and distinction between collaboration and cheating
- **Iterative Development:** Create living policy document that evolves as technology advances, with regular review cycles and feedback mechanisms [11]

Policy Implementation Roadmap

Successful AI policy implementation requires structured rollout with training and clear communication

- **Cross-Department Leadership**: Establish team including curriculum, IT, legal, student services, and teaching representatives to guide AI integration [11]
- **Connect to Existing Policies**: Update current acceptable use, technology procurement, and data privacy policies rather than creating isolated AI documents [11]
- **Professional Learning Priority**: Provide ongoing training for educators on responsible AI use, tool evaluation, and integration strategies - not one-time workshops [11]
- **Transparent Communication**: Educate students, parents, and community about AI policies, benefits, and safeguards through multiple channels [11]

Phase 1 - Foundation

Form AI leadership group, conduct needs assessment, review existing policies

Phase 2 - Development

Draft policy with stakeholder input, establish vendor vetting procedures

Phase 3 - Training

Professional development for staff, student AI literacy programs, parent communication

Phase 4 - Pilot

Small-scale testing with specific grades or subjects, gather feedback and adjust

Phase 5 - Rollout

District-wide implementation with ongoing support and monitoring

Phase 6 - Continuous Improvement

Regular policy review, emerging tool evaluation, refinement based on experience

AI Architecture Fundamentals

Understanding AI data architecture is critical for protecting student information and maintaining security

- **Data Pipelines:** AI tools connect to multiple district systems simultaneously, creating complex data flows [14]
- **API Security:** Interfaces linking AI to student data must use encryption and authentication controls [14]
- **Local vs Cloud Processing:** Understand whether data is processed locally or transmitted to cloud servers [14]
- **Data Residency Questions:** Know where student data physically resides and which jurisdictions govern it

Connection Point	Data Access
Student Information Systems	Direct integration with demographic and academic data
Learning Management Systems	Access to assignments, grades, and interaction patterns
Authentication Systems	Single sign-on and identity management connections
Communication Platforms	Email and messaging system integrations
Assessment Tools	Test results and performance analytics integration

Source: How to Secure AI Tools Within Your K–12 Digital Envir...

AI Gateways & APIs: Controlling What Data AI Agents Can Access

AI agents decide what to access dynamically, chain tools autonomously, and generate queries you didn't pre-write

AI agents do not inherently understand data sensitivity, business context, or authorization boundaries

AI agents are non-human principals requiring their own identities, credentials, policies, and audit trails

Most AI breaches happen because agents accessed too much data and APIs returned unfiltered responses

- **Definition:** An AI gateway is a control plane that sits between an AI agent and data/tools, enforcing policy, visibility, and constraints on what the agent can access and do
- **Core Problem Solved:** AI agents do not inherently understand data sensitivity, business context, or authorization boundaries, so we must externalize control through gateway enforcement
- **Control Method - Scoped APIs:** Instead of Agent to Database, use Agent to API to Filtered Response where the API applies row-level security and enforces business logic



Panorama Solara

Make student support easier with secure AI that's customizable to your district's goals and practices.

Secure AI Platform Purpose-Built for K-12

2,000+
Districts [17]

500+
Districts Using AI Tools [17]

SOC 2
FERPA, COPPA Compliant [17]

- Purpose-built AI chat tool designed for K-12 districts, combining innovations with 12+ years of educational expertise [17]
- Securely integrates with Skyward SIS and Panorama data for real-time student insights grounded in actual data [17]
- Creates intervention plans, lesson plans, and IEP accommodations tailored to each district's curriculum and materials [17]
- Student information never used to train AI models, providing full confidence in data privacy and security [17]
- Built on AWS using Claude AI, processing 380,000+ student records across 25 states with comprehensive dashboards [18]



Mesquite ISD Transforms Special Education with AI

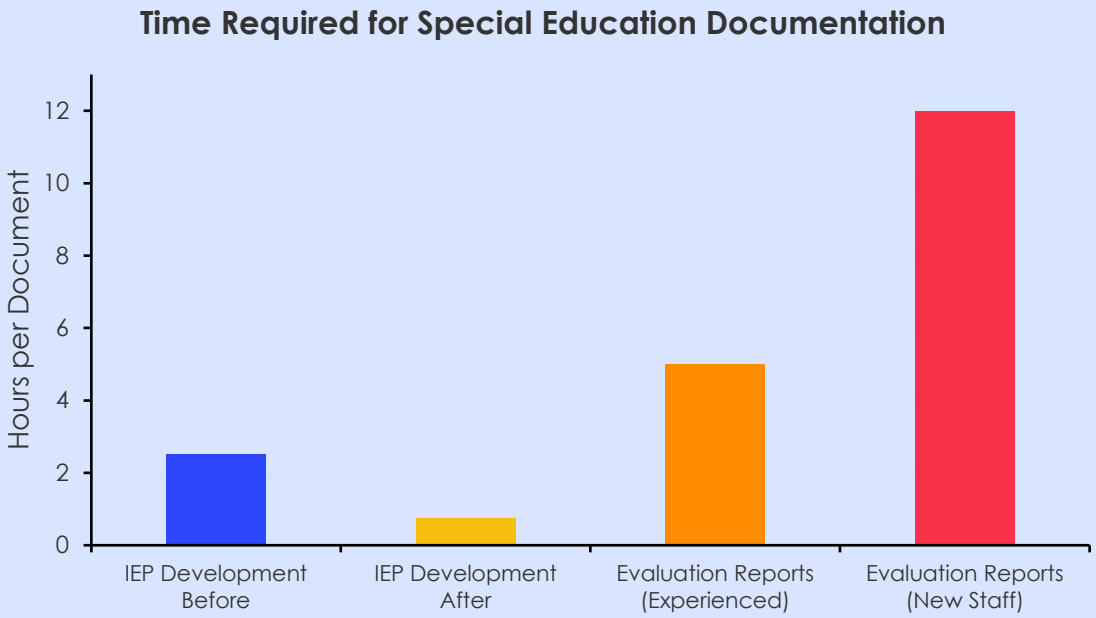
Texas district serving 36,000+ students dramatically reduces documentation burden while improving IEP quality through Panorama Solara and Skyward integration

36,000+
students served [19]

52
campuses district-wide [19]

45 min
IEP drafting time (from 2-3 hours) [19]

- Partnered with Panorama to implement Solara AI platform for special education alongside Student Success system
- Skyward integration connects data across systems for timely interventions without manual transfer [19]
- Supports Texas HB 1416 requirements while maintaining FERPA-compliant data privacy standards [20]



Source: AI in Special Education: How Mesquite ISD Uses Panora...

From Hours to Minutes: Special Education Transformation

- **Challenge:** Writing IEPs required 2-3 hours per student with manual data gathering from disconnected systems [19]
- Time constraints led to generic plans with less impactful interventions and untapped student growth potential
- **Results:** IEP drafting time reduced to 45 minutes, allowing educators to reclaim time for student interaction [19]
- Students receive more individualized IEPs and 504 plans grounded in comprehensive current data rather than templates

Lessons from Early Adopters

Common patterns emerge from successful AI implementations across diverse school contexts [21]

- Start Small and Specific: Most successful districts began with single pain point (communication, lesson planning, data analysis) rather than comprehensive AI transformation [21]
- Personalized Learning Gains: Adaptive AI platforms analyzing individual student patterns enable teachers to adjust instruction in real-time, though human oversight remains essential [1]
- Administrative Efficiency: AI automation of scheduling, attendance, grading creates time for educators to focus on teaching and student relationships [21]
- Data-Driven Decision Speed: AI-enabled dashboards provide principals with weekly actionable data, allowing faster resource adjustments and intervention targeting [21]
- Teacher Training Non-Negotiable: Technology alone doesn't drive success - ongoing professional development and support determine whether AI tools deliver value or gather dust
- Combined Human-AI Model: Research shows students with both human and AI tutoring advance 0.36 grade levels more annually than AI-only support [22]

Assess Current State

Inventory existing AI tools already in use, survey staff needs and concerns

↓

Build Your Team

Form cross-functional AI leadership group with diverse representation

↓

Develop Policy Draft

Start with framework addressing safety, privacy, and acceptable use

↓

Pilot Strategically

Select one high-value, low-risk use case for initial implementation

↓

Evaluate and Iterate

Gather feedback, measure outcomes, adjust approach based on learning

Your Action Plan

- **Don't Wait for Perfect**: Start with strong principles and clear boundaries, learn as you implement [23]
- **Leverage Existing Resources**: Use state guidance, CoSN frameworks, and peer policies as starting points [11]
- **Focus on Quick Wins**: Target administrative tasks that consume teacher time for early applications [21]
- **Vendor Vetting Checklist**: Systematic evaluation of security certifications, privacy policies, and compliance [24]
- **Communicate Proactively**: Address staff concerns upfront, positioning AI as tool enhancing expertise
- **Measure What Matters**: Define metrics before implementation - time saved, outcomes, satisfaction



Preparing for an AI-Powered Future

AI literacy is becoming essential job skill for students, requiring districts to balance innovation with protection

- **Workforce Preparation:** Students will work alongside AI daily - K-12 exposure builds critical literacy and judgment skills
- **Student AI Literacy:** Teach safe, legal, ethical AI interaction through scaffolded experiences and explicit instruction [11]
- **Evolving Threat Landscape:** As AI advances, risks grow - continuous policy review and tool evaluation becomes ongoing responsibility
- **Equity Imperative:** Ensure AI benefits reach all students, avoiding digital divide and literacy advantages gaps
- **Federal Guidance Coming:** Executive order establishes national AI Education Task Force, signaling increased federal involvement and resources [23]
- **Your Leadership Matters:** IT leaders shape next generation's AI experience - prioritize safety and ethics while enabling innovation

Skyward's IT experts have the latest knowledge on industry trends and developments to help keep your network running smoothly.

NETWORK CONSULTING

- Resilient Wired Network Infrastructure
- Complete Wireless Network Solutions
- Virtual Server Design and Support
- Storage Area Network Solutions
- IP Telephony Solutions

SUPPLEMENTAL IT STAFFING

- Onsite and Remote IT Support
- Network Assurance Services

ASSESSMENT SERVICES

- Network / Security
- Disaster Recovery
- Secure Cloud Computing

SKYWARD OPTIMIZATION

- Managed Services
- Database Tune-ups
- Remote Update Services
- System Admin Training

NETWORK SECURITY SOLUTIONS

- Intrusion Detection, Prevention, and Next Generation Firewalls
- Email Filtering, Archiving, and Security Solutions
- Internet Filtering and Monitoring Solutions
- On-Staff Security Experts

DISASTER RECOVERY SERVICES

- Skyward Disaster Recovery from ISCorp
- Onsite Data Center Disaster Recovery Solutions

SKYWARD®

iCON

thank you!

References

#	Link
1	https://www.linkedin.com/pulse/ai-k12-classrooms-tools-case-studies-implementation-jacob-brewer-6wzve
2	https://www.panoramaed.com/blog/ai-security-concerns-in-education
3	https://mljourney.com/probabilistic-vs-deterministic-machine-learning-algorithms-understanding-the-fundamental-divide/
4	https://mitsloanedtech.mit.edu/ai/basics/addressing-ai-hallucinations-and-bias/
5	https://oboe.com/learn/probabilistic-vs-deterministic-ai-outputs-bwalo8
6	https://www.alphanome.ai/post/probabilistic-vs-deterministic-models-in-ai-ml-a-detailed-explanation
7	https://www.lightspeedsystems.com/challenges/student-safety-wellbeing/ai-risks-and-safety-in-schools/
8	https://www.securityinfowatch.com/cybersecurity/article/55305312/how-to-safeguard-k-12-schools-in-the-age-of-ai
9	https://www.newamerica.org/oti/blog/artificial-intelligence-in-schools-privacy-and-security-considerations/
10	https://studentprivacycompass.org/state-guidance-on-the-use-of-generative-ai-in-k-12-education/
11	https://ospi.k12.wa.us/sites/default/files/2024-06/comprehensive-ai-guidance.pdf
12	https://www.clever.com/blog/2024/01/edtech-vendor-security

References

#	Links
13	https://ctl.net/blogs/insights/beyond-the-hype-the-k-12-directors-framework-for-vetting-ai-solutions
14	https://edtechmagazine.com/k12/article/2025/05/how-secure-ai-tools-in-k12-environment-perfcon
15	https://smoothwall.com/resources/managing-access-to-ai-tools-with-web-filtering
16	https://www.magicschool.ai/ai-policy/usage-guidelines
17	https://www.panoramaed.com/products/ai/panorama-solara
18	https://aws.amazon.com/blogs/publicsector/unlocking-student-success-with-generative-ai-how-panorama-education-built-solara-on-aws/
19	https://www.panoramaed.com/blog/mesquite-isd-special-education
20	https://www.skyward.com/about/newsroom/skyward-partners-with-panorama-to-bring-leading-ai-and-intervention-solutions-to-texas-districts
21	https://www.edelements.com/blog/how-ai-is-powering-everyday-school-improvement-5-real-examples-from-districts-nationwide
22	https://schoolai.com/blog/ai-tools-in-education
23	https://www.teachingchannel.com/k12-hub/ebook/ai-policy-and-implementation-guide-for-k-12-schools/
24	https://www.sreb.org/publication/ai-tool-procurement-implementation-and-evaluation-checklist