State Guidance on AI Use in K-12 Schools: Data Privacy Considerations (Updated 4/29/2025)

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
Alabama	-Data usage -Data storage -Data processing -Data security	-Acknowledges the importance of data privacy concerns associated with AI use in schools -Ensure compliance with existing state and federal privacy laws -Ensure appropriate usage of data data collected by AI tools, including requiring that it is not being used to train new AI systems -Vet new AI products before implementation -Includes model contract language	"The primary goal . . . will be achieved by focusing on AI governance, accountability, safety, procurement and implementation, data privacy and security, data quality concerns, bias, responsible use, transparency, access, efficacy, AI knowledge, skills, education, and training." "The (replace with name of LEA) is committed to complying with federal, state, and local laws, rules, and regulations, and other entities that provide standards for compliance to ensure data privacy and security are maintained for data used in AI systems. We will ensure that the Contractor's AI systems comply with all applicable federal, state, and local laws, rules, and regulations, and other entities that provide standards for compliance." "The (replace with the name of LEA) is dedicated to ensuring data to be used in the AI systems will meet the data quality standards established by our	[none mentioned in guidance]

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			Data Governance Committee." "Use of user's data to train new AI Systems: The (replace with the name of LEA) will include in our procurement and contract document(s) verbiage (Appendix A), which the Contractor shall attest when submitting their proposals and any contract executed to perform the work." "The (replace with the name of LEA) will conduct a detailed needs and capability assessment before procuring an AI system. We will evaluate the AI system for its effectiveness, ease of use, and compatibility with existing systems. In the procurement process, we will consider cost, data privacy, security, human-in-the-loop development, algorithm bias, model cards, system cards, interoperability, service-level agreements, key performance indicators, customizability, configurability, scalability, legal compliance, and contractor support." "The (replace with the name of LEA) will obtain a written statement from contractor that: 1. The AI model(s) have been	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			pretrained and no data is being used to train a model to be used in the development of a new product. 2. Have been responsible in the development of the AI systems by using human-in-the-loop during model development; have taken steps to minimize bias to the extent possible in the data selection process and the algorithm development; and the results have met the expected outcomes." "The Contractor hereby attests and agrees that it is expressly prohibited from using any data provided to it by the data providers—either in its raw form or after undergoing any form of processing, aggregation, or transformation—for the purpose of training a new AI System to be used in a new product, model, service, or offering (collectively referred to as the "Product") of the Contractor." "Details of Data Use: The RFA shall include a comprehensive written explanation that outlines the following, but is not limited to: Purpose of data usage.	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			Data elements that will be used for the AI System training. Specifics of the AI System. Methods of data utilization. Expected outcomes. Duration of data usage. The manner the data providers' data will be stored, processed, and secured. Name(s) of the individual(s) who will have access to the data. The controls in place to prevent unauthorized use. Specific types of data that will be used for model training. Description of the model training process. Risks associated with using the data for model training and how these risks will be mitigated. A risk register contains the following, but is not limited to: Level of risk. Mitigation strategies. Status of the risk(s)."	
Arizona	-Data protection/data security -Misuse of data	- Acknowledges data privacy risks of AI in education and recommends transparency in data privacy practices surrounding AI usage	"An LEA's compliance with student privacy laws may be put at risk by using certain tools and applications in a school setting. • Introducing AI in the school environment may raise	ARS 15-142 ARS 15-117 ARS 15-1046

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			questions from parents and families regarding the protection of their children's data. • Problems can occur if data that was used as GenAI input for a specific purpose is later used in a different application. For example, data collected for research and then repurposed for commercial purposes is considered data misuse. • GenAI tools and platforms may be susceptible to security breaches, hacking attempts, or unauthorized access which could compromise the confidentiality and integrity of student data."	
California	-Data protection and security -Data collection, storage, and retention - Data ownership - Access and sharing data	-Ensure compliance with existing state and federal privacy laws -Thoroughly evaluate Terms of Use for AI products -Omit student PII when inputting data into AI systems	"As school districts consider the integration of AI systems into their educational environments, it is essential to thoroughly evaluate the terms of use to ensure the responsible and effective deployment of AI technology." "It is vital that educators omit identifiable student information when	CA CIVIL 1798.29; CA 1798.82 CA EDUC 49073.1 CA BUS & PROF § 22584 & CA BUS & PROF § 22585

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
		-Vet AI system's data handling for adherence to privacy protocols -Clarify ownership of data generated or processed by the AI system -Establish rights and responsibilities regarding data access and sharing -Ensure the AI system's adherence data retention policies -Assess AI system's data security	inputting data to AI systems. It is important that educators and students review when and if data they input into an AI system is collected, and if that data will be stored to further its learning or be deleted." "Districts and educators must consider COPPA (Children's Online Privacy Protection Act) and FERPA (Family Educational Rights and Privacy Act) when considering AI use in the educational setting." "Data Handling: Review how the AI system collects, stores, and manages student data. Ensure it adheres to privacy protocols and encryption standards." "Data Ownership: Clarify who owns the data generated or processed by the AI system and establish rights and responsibilities regarding data access and sharing." "Data Retention: Determine how long the AI system retains student data and whether it aligns with your district's data retention policies."	CA EDUC § 49073.6 CA EDUC 49076.7 (2016): CA BUS & PROF 22586

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			"Data Security: Assess the AI system's security measures, including encryption, authentication, and authorization protocols, to safeguard against data breaches and cyber threats."	
Colorado	-Data usage -Data storage -Data sharing	-Regular policy and vendor contract reviews and augmentation -Transparency surrounding data usage, storage, and sharing -Ensure AI system's compliance with existing privacy laws	"Regular policy and vendor contract review will be ongoing. In doing so, understanding the data usage in AI model training is crucial, as policies must reflect the iterative and generative nature of AI tools. This involves proactively using certain student information to train AI tools while ensuring bias elimination. Transparency in how data is used to produce outputs from prompts is essential. Clear communication about what data is being used, its storage duration, and data sharing practices with subcontractors or partners enhances data transparency. Additionally, considering how APIs function as gatekeepers for data usage by providers is vital for effective data utilization. " "Review and augment existing data	CO REV ST 22-16-101-112 CO REV ST 22-16-101-112

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			privacy policies and vendor agreements." "Colorado's unique local control context empowers local school districts to adopt their own policies, limiting the state department of education's ability to dictate local technology policies. Even so, Colorado's current Student Data Privacy rules are among the most protective in the nation. The policies and practices to safeguard students largely already exist, and can benefit from regular review as technology advances. Because policy guidance stretches across multiple areas related to AI in education, we offer the following guiding tenets as prudent for school districts to begin with."	
Connecticut	-Data collection	-Schools should assess the breadth and type of data that AI-powered tools collect. -Adhere to existing state and federal privacy laws	"Privacy and Data Collection: As part of the selection process and in ongoing use, schools should assess the breadth and type of data that AI-powered tools collect. Public	Special Act 18-28 CT Gen St 10-234aa CT Gen St 10-234bb

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			schools must adhere to Connecticut's data privacy laws, with guidance on doing so available through the Commission's Student Data Privacy Web page. The Connecticut Educational Software Hub, powered by LearnPlatform, offers details on thousands of instructional apps to assist with this process." "Members of the Data & Privacy Advisory Council of the Connecticut Commission for Educational Technology assembled a list of research and resources to assist K-12 school districts adopt best practices regarding protection of student data accessible to third parties" "Educators and district leaders can search for educational software developed by companies that have pledged compliance with Connecticut's privacy law" "Federal legislation and guidance	CT Gen St 10-234bb CTPA 19-146

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			governing educational technology and student privacy (CIPA, COPPA, FERPA, and IDEA)"	
Delaware	-Data collection -Data protection and security -Data storage -Data access and sharing -Data usage	-Implement strict data privacy and security measures -Adhere to existing state and federal privacy laws -Do not manually enter PII into Generative AI systems -Ensure the Generative AI vendor complies with signing Delaware Department of Technology & Information (DTI) Terms and Conditions Governing Cloud Services and Data Usage. -Ensure AI systems are safe -School Districts and Charter Schools must prioritize establishing robust data governance policies with precise data collection, storage, access, and sharing protocols. -Establish transparency with students and parents about using	"Privacy Concerns: the use of AI in education involves collecting and analyzing vast amounts of personal data from students, raising significant privacy concerns." "Protecting student data: implement strict data privacy and security measures to protect information and data, adhering to laws such as FERPA, COPPA, CIPA, IDEA, and Section 504 where applicable." "Protecting Student Data: Establish strict data privacy and security measures to protect PII, especially student information" "Personally Identifiable Information (PII) should not be manually entered into Generative AI systems. Adhere to federal and state laws. Ensure the Generative AI vendor complies with	SB 79 SB 208

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
		Generative AI and the data it generates. -Provide students and parents accessible information on how data is used to support educational goals and how privacy is protected. -School districts should consider implementing professional learning for educators on Generative AI in the classroom, including surrounding data privacy and protecting student data. -Investigate how the tool/system will specifically be implemented in your context and what data will be collected from which parties for what purposes. -Ensure that no extraneous data is being collected, data is not surviving the intended purpose, and that data is not retained beyond its useful life.	signing Delaware Department of Technology & Information (DTI) Terms and Conditions Governing Cloud Services and Data Usage. Ensure AI systems are safe, minimizing risks to humans" "School Districts and Charter Schools must prioritize establishing robust data governance policies with precise data collection, storage, access, and sharing protocols. Implementing these tools should be accompanied by rigorous security measures, including encryption and secure authentication, to safeguard against unauthorized access to sensitive information. Furthermore, transparency with students and parents about using Generative AI and the data it generates is crucial. This involves providing accessible information on how data is used to support educational goals and how privacy is protected. By thoughtfully integrating technologies within a framework of strong data protection practices, academic institutions can	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			unlock the potential of Generative AI to personalize learning while simultaneously upholding the trust and confidence of the educational community in the digital age." "Professional Learning Programs These offerings below highlight examples for consideration when implementing your school district or charter school's professional learning for educators on Generative AI in the K-12 classroom: . . . Protecting Student Data Prompt Engineering for Educators: Best practices for designing prompts that maximize teacher capacity while protecting student data and PII. Generative AI to Support Pedagogy: Leverage tools for personalized learning, student engagement, and formative assessment to enhance classroom pedagogy and support individual student needs while maintaining student data privacy." "The Emerging Technology Adoption Framework Data Privacy section:	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			- "Investigate how the tool/system will specifically be implemented in your context and what data will be collected from which parties for what purposes - Ensure that no extraneous data is being collected, data is not surviving the intended purpose, and that data is not retained beyond its useful life"	
Georgia	- Data minimization practices -Data collection, security, and sharing	-Acknowledges importance of data privacy surrounding AI use in schools and its associated risks -Ensure compliance with existing state and federal privacy laws - Use data minimization practices such as not inputting PII into AI applications and using anonymized or aggregated data -Establish formal agreements with AI vendors to protect student data privacy -Educate staff and students on AI	"Respect privacy and ensure data protection in all AI endeavors." "To protect Personally Identifiable Information (PII), the following practices must be adhered to: • Never input PII, such as social security numbers, home addresses, health information, academic information, employee performance, or other sensitive data into AI systems.	Children's Online Privacy Protection Rule (COPPA): • 47 USC §231 • 16 CFR Part 312 Family Educational Rights and Privacy Act (FERPA): • 20 USC §1232g

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
		data privacy best practices	• Utilize anonymized or aggregated data (utilizing a locally determined n size) whenever possible so specific students and staff cannot be identified. • Educate all users about the risks and responsibilities of handling PII and integrate this into annual professional learning requirements. Protecting student and staff privacy is a top priority. AI systems can process vast amounts of data, and it is essential to ensure that this data does not include sensitive personal information. Schools should implement strict data handling policies and provide training to all staff on data privacy best practices." "How have AI and PII best practices been integrated into annual student privacy professional learning for all educators and staff? 2. Are all district staff trained on the	• 34 CFR Part 99 Privacy Act of 1974: • 5 USC §552a • 22 CFR Part 1101 Protection of Pupil Rights Amendment (PPRA): • 20 USC §1232h • 34 CFR Part 98 Section 504: Rehabilitation Act IDEA (Individuals with Disabilities Education Act):

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			importance of protecting personal and private information when interacting with AI systems? 3. Is there a monitoring process to ensure compliance with data privacy practices and federal regulations?" "Districts and schools should establish formal agreements with AI vendors to protect the school district, staff, and students, which should include . . . Data privacy and security commitments from the vendor." "TrustEd Apps is a catalog of applications and software vetted for use. Each application in the catalog has been researched and validated to ensure security and data privacy. The TrustEd Apps data privacy rubric examines four key areas: data collected, security, third-party sharing, and advertising" "Compliance with privacy laws and regulations, data encryption, and	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			anonymization practices."	
Hawaii	-Data collection -Data usage	-Assess AI tools' terms of use and privacy policies to identify risks with data collection and use -Obtain approval from school administration and state offices -Avoid entering PII into AI tools	"Read through terms of use and privacy policy before using AI tools to identify risks with collected data and its use" "Obtain necessary approval from school administration and state offices" "Avoid entering personally identifiable information (PII) into AI tools"	SB2607
Indiana	-Data protection and security	-Do not input PII into public-facing AI tools -Create policies for AI implementation -Ensure compliance with local policies and state and federal laws\ -Develop a space where educators can practice making decisions about AI security issues	"Ensure inputs into public facing AI tools are free from personal identifiable information (PII)." "Create a use policy to address best practices when making decisions about AI implementation." "Follow local policies regarding student data. Ensure compliance with FERPA/COPPA before using AI with students."	[not listed in guidance]

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			"Develop a "sandbox" where educators can practice making decisions about security issues related to AI."	
Kentucky	-Data security	-Ensure adherence to state and federal privacy laws -Continually develop AI data best practices	"All AI application usage should adhere to state and federal privacy laws, such as the Family Educational Rights and Privacy Act (FERPA)[5], the Children's Online Privacy Protection Act (COPPA)[6], and Kentucky House Bill (HB) 5 (2015)[7]. Student and educator data should always be treated with utmost confidentiality and security." "The KDE will hold to our data governance and data quality standards and partner with experts when appropriate to identify continued development of data best practices when using created or curated AI systems."	HB 232

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
Louisiana	-Data use and storage -Data security -Data sharing agreements	-Acknowledge importance of data privacy and AI use -Ensure compliance with existing privacy laws -Carefully craft data-sharing agreements with vendors who use AI in their tools -Establish student data privacy protocols	"Data Privacy and Security: Robust data privacy and security measures must be in place to protect student information and ensure compliance with relevant regulations." "School leaders should be aware of federal regulations like FERPA and COPPA and statespecific data privacy laws, such as the Louisiana Student Privacy Law (R.S. 17:3914) (See Relevant Laws and Policies). The school system must implement secure data storage practices, obtain parental consent when necessary, and provide transparency when AI systems collect, process, and utilize student data." "Closed system applications refer to software or platforms operating within a controlled environment, often without an internet connection. Closed-system AI applications are preferred in educational settings because they provide greater control over data privacy and security"	FERPA LA R.S. 17:3884 CIPA COPPA IDEA LA R.S. 17:3921.2 LA R.S. 17:3913; LA R.S. 17:3914 Section 504 Rehabilitation Act Title VI of the Civil Rights Act of 1964 Equal Educational Opportunities Act of 1974 Bulletin 110

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			"In compliance with R.S. 17:3913, Data-Sharing Agreements (DSAs) between AI vendors and LEAs must be crafted to ensure compliance with privacy regulations and safeguard sensitive student information, including video and audio recordings, among other data. The LDOE website provides more details regarding DSAs." "Educational technology personnel should prioritize data privacy and security related to AI technologies. Protocols should be established and maintained to protect student data and ensure compliance with federal and state laws. LDOE Digital Learning provides helpful resources for cybersecurity incident prevention"	Bulletin 104
New Jersey	[contains links to other resources, some of which briefly mention data privacy as an AI risk]	[no clear recommendations regarding data privacy and AI outside of linking to other resources]		A4978

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
North Carolina	-Data usage, storing, and sharing -Data protection and security	-Do not input student PII into an AI tool -Prioritize technologies that comply with state, federal, and local laws regarding data privacy and security in educational settings -Establish transparent, best-practices-aligned policies and communicate to students, parents, and educators how data collected by AI technologies will be used, stored, and shared. -Verify security standards of third-party vendors	"All users must be taught the importance of protecting data privacy when using generative AI tools. Users should never input Personally Identifiable Information or PII. into an AI tool (or anywhere else without careful consideration)!!! Student ID Numbers are PII. Be especially mindful of this when pasting data into the model or uploading any data that may contain PII." "FERPA defines the term PII to include direct identifiers (such as a student or other family member's name) and indirect identifiers (such as a student''s date of birth, place of birth, or mother's maiden name)" "All users should be reminded of what data is considered PII, and that includes student ID numbers. Users should use caution in particular to avoid inadvertently copying or uploading PII into the model when	[not mentioned in guidance]

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			evaluating student responses, analyzing data, or creating personalized content such as IEP goals, personalized learning plans, etc." "Prioritize technologies that comply with federal, state, and local regulations regarding data privacy and cybersecurity in educational settings. Familiarize yourself with regulations like the Family Educational Rights and Privacy Act (FERPA) in the United States and similar laws in other regions." "Clearly communicate to students, parents, and educators how data collected by AI technologies will be used, stored, and shared. Establish transparent policies that align with best practices for data privacy in educational settings." "If using third-party platforms or services, verify that the vendors adhere to stringent security standards. This includes	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			evaluating their data protection policies, encryption practices, and overall commitment to cybersecurity. “	
North Dakota	-Data protection and security	-Review and vet current EdTech providers -Ensure AI tool’s compliance with privacy laws and policies -Ensure understanding of how an AI tool protects student and staff data -Review how an AI tool communicates data breaches	“ Review current EdTech providers supplying AI to vet their safety, privacy, reliability, and efficacy to determine if they are appropriate for your school and which users they will support based on their terms of service” “Implementation checklist: evaluate privacy and security concerns of the tools: - Does the tool comply with privacy laws (FERPA, HIPAA)? - Does the tool comply with local privacy policies? - Understand how the tool protects students’ and staff’s data. - How does the tool communicate data breaches?	SB 815 HB632

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
Minnesota	-Data security -Data collection, storage, and use	-Consider how use of AI can fit into existing policy frameworks for data privacy -Data privacy and security should be a primary consideration when adopting new technology -Robust privacy policies and safeguards are required surrounding student data collection, storage, and use	"Data privacy, security and content appropriateness should be primary considerations when adopting new technology. Consider existing policies related to these issues and how the use of AI fits into existing frameworks." **"**Data Privacy and Security: Ethical concerns surround student data collection, storage, and use, requiring robust privacy policies and safeguards."	Minn. Stat.13.32 HF No. 2353
Mississippi	-Data security -Data sharing	-Teachers should be familiar with the privacy policies of AI tools -Administrators should offer guidance and support to staff on protecting student privacy -Follow existing federal privacy laws	"Cautions: Increase data privacy and security risks depending on the technology provider's privacy and data sharing policies" "Teachers: Be familiar with age restrictions and privacy policies of AI tools." "Administrators: Offer guidance and support to staff on protecting student privacy, including COPPA and FERPA guidelines, regarding student	[none mentioned in guidance]

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			use of digital tools and data shared with AI platforms."	
Ohio	[links to resources, some of which mention data privacy risks at a high level]	[no clear recommendations regarding data privacy and AI within the guidance itself; does provide other resources]		SB 29
Oklahoma	-Data protection and security	-AI applications that collect more and more sensitive student PII pose a higher risk to data privacy and security and should be used with extreme caution; AI applications that collect less data should still be used with caution and one should ensure responsible use	"Potential risks: compromised student privacy and unauthorized data collection" "Low risk: ensure responsible use. AI tools and applications that do not require the use of personally identifiable information (PII). Implementing data anonymization and security measures can help mitigate residual privacy risks" "Medium risk: use with caution. AI applications that collect personal data such as learning analytics, engagement metrics, and assignment feedback. Enhanced security	[none mentioned in guidance]

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			protocols, transparent data practices, and clear communication on usage expectations can help mitigate these risks." "High risk: use with extreme caution. AI applications that collect sensitive information, like student demographics or personal identifying information. It is crucial to implement robust security measures, strict adherence to user consent, and continuous data monitoring may help mitigate these risks."	
Oregon	-Data use	-Use caution when entering personal information into generative AI applications -Review data use policies and privacy policies	"Users should be cautious when entering personal information into any technology application. This is a particularly important consideration when using generative AI applications such as ChatGPT as the information entered by users (including prompts and questions posed) is stored on the application's server and integrated into the large language model used to respond to user prompts." "Whenever new technology is	HB 1989 HB 2784 HB 1506

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			introduced, reviewing the data use and privacy policies are of key importance.”	
Utah	-Data collection -Data use	-Do not enter sensitive information when using AI models -Do not enter private or confidential data to a publicly accessible AI service or training model -Sensitive material shall not be interred into generative AI models that have not been approved for that use case -Contracts shall prohibit vendors from using State of Utah materials or data in generative AI queries or for building or training proprietary generative AI programs unless explicitly approved by the state. - The use of AI is required to adhere to state and Federal privacy laws.	“Sensitive information. When using AI or using AI models, do not enter or share sensitive information or files. Indicate the level of sensitivity by following the “sensitivity label” protocol to be established in the near future. “ “ No private, controlled, or confidential data shall be added to a publicly accessible AI service or training model. “ “Material that is inappropriate for public release shall not be entered as input to generative AI tools that have not been explicitly approved for the intended use case.” “Agency contracts shall prohibit vendors from using State of Utah materials or data in generative AI queries or for building or training proprietary generative AI programs	SB226 HB 163 SB 204 HB358 SB102 SB 163 SB207 HB 27 HB 28 SB164 SB 166

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
		-No use of AI in ways that compromise teacher or student privacy or lead to unauthorized data collection -AI tools must detail if/how personal information is used -Entering confidential or personally identifiable information into unauthorized AI tools is prohibited	unless explicitly approved by the state." "Privacy concerns: The use of AI is required to adhere to state and Federal privacy laws." "Compromising Privacy: The education system will not use AI in ways that compromise teacher or student privacy or lead to unauthorized data collection, as this violates privacy laws and our system's ethical principles. See the Security, Privacy, and Safety section below for more information." "Noncompliance with Existing Policies: We will evaluate AI tools for compliance with all relevant policies and regulations, such as privacy laws and ethical principles. AI tools will be required to detail if/how personal information is used to ensure that personal data remains confidential and isn't misused. " "Staff and students are prohibited from entering confidential or	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			personally identifiable information into unauthorized AI tools, such as those without approved data privacy agreements. This extends to contracted vendors and other third parties. Sharing confidential or personal data with an AI system could violate privacy if not properly disclosed and consented to."	
Virginia	-Data protection	-Ensuring privacy is protected will be a guiding principle	"Ongoing roles and responsibilities: Safeguarding privacy, security, and confidentiality of data" "Do no harm: This includes ensuring the safeguarding of the privacy, security, and confidentiality of personally identifiable information, ensuring that algorithms are not based on inherent biases that lead to discriminatory outcomes"	HB1 SB 242 HB 1334 HB 1612 HB 1698 HB 2350 SB 438 HB519 HB 749

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
				HB 750 SB951 HB2449 SB 764 ER
Washington	-Data protection and security -Data deletion and opt-out	-Ensure AI use complies with applicable laws -Update policies to include the use of and considerations for using AI. Give users options to opt-out or delete their data if they want. -Support technology leadership in addressing risks of data breaches and external sharing of student or staff information. -Review implemented software that does not promote student profiling and surveillance. -Provide students with	"Ensure that your LEA AI use complies with student/personal privacy and data protection laws. Be aware of and follow any age restrictions for the use of all AI tools and resources. Before sharing private data, ensure that the AI tool meets the following requirements: FERPA, COPPA, CIPA." "Have a clear understanding of your data collection processes. Update policies to include the use of and considerations for using AI. Give users options to opt-out or delete their data if they want."	SB 5419

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
		grade-level appropriate instruction in thinking critically about their digital security -Lead the vetting of AI tools: ensure software companies' Data Privacy Agreements (DPAs) are verified; validate that companies are COPPA, CIPA, and FERPA compliant, including security requirements; confirm that the vendor software follows best practices in protecting student data -Prioritize security and data privacy. -Implement vetting procedures requiring vendors to notify the district when updates including AI changes are made.	"Sample student AI code of conduct: Protect Privacy: I will be mindful of my own and others' privacy when using AI. I will not share personal information with AI without appropriate consent and understanding of how the data will be used" "Sample professional ethics for educators when implementing AI tools: protect student privacy and data ● Establish safeguards to make certain that student data collected, used, and stored is secure and with appropriate consent. ● Confirm that any data collected does not violate current regulations relevant to education and student data privacy" "LEAs and Student Privacy and Data Security: Continue to evaluate the need to	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			balance data demand with student privacy concerns. Continue to support technology leadership in addressing risks of data breaches and external sharing of student or staff information. Continue to review implemented software that does not promote student profiling and surveillance. Provide students with grade-level appropriate instruction in thinking critically about their digital security" "Lead the vetting of AI tools: ensure software companies' Data Privacy Agreements (DPAs) are verified; validate that companies are COPPA, CIPA, and FERPA compliant." "Information technology/educational technology leaders: security and privacy: Prioritize security and data privacy. Implement vetting procedures requiring vendors to notify the district when updates include AI changes are made. Ensure that the software's security features and encryption comply with	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			regulations (e.g., FERPA, CIPA, and COPPA). Confirm that the software vendor follows best practices in protecting student data."	
West Virginia	-Data collection -Data protection and security -Parental consent -Data use	-Do not use AI in ways that could compromise teacher or student privacy or lead to unauthorized data collection -Evaluate AI systems for compliance with relevant laws -Obtain parental consent and inform parents of data collection and use -Using PII in public AI models is not advisable -Implement security against unauthorized access and misuse -Train staff on AI and cybersecurity -Never input PII into AI systems without authorization	"The county school district or school will not use AI in ways that compromise teacher or student privacy or lead to unauthorized data collection, as this violates privacy laws and our system's ethical principles. WVBE Policy 2460 requires that counties are responsible for ensuring that COPPA, CIPA, and FERPA are not violated." "Obtaining parental consent is crucial, but it is also important to recognize that even with consent, using identifiable data in public AI models is not advisable." "Schools should implement reasonable security measures to secure AI technologies against unauthorized access and misuse. These measures may include (1)	HB4261 HB 4316

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			cataloging the tools used, their purposes/functions, and the information required (e.g., information about individuals, prompts or questions, aggregate data); (2) establishing rules or criteria for who can use AI tools for what purposes and/or creating school-specific guidelines for use of AI tools; and (3) maintaining up-to-date information about the technical details and security implications of the tools in use. All AI systems deployed within the school should be evaluated for compliance with relevant laws and regulations, including those related to data protection, privacy, and students' online safety. Schools and districts should also ensure that staff are adequately trained for how to securely and successfully use AI tools from both cybersecurity and instructional perspectives." 'Data Collection: Parents, guardians, and students will be informed of specific data	

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			collection initiatives, and where applicable, consent will be sought. All AI-driven data collection will adhere to local data protection regulations and best practices." "Third-Party AI Tools: Schools may develop an approved list of AI tools which should always be consulted. Unauthorized AI tools might not adhere to data privacy standards." "Personal Information: Staff and students should never input personal, sensitive, or confidential data into any AI system without prior authorization, including any data related to student education records."	
Wisconsin	-Data privacy generally	-Review and update existing policies to reinforce data privacy concerns -Protecting user data privacy is paramount to successful AI usage	"Districts should review existing policies and processes to incorporate AI-related language that reinforces ethical considerations as well as data privacy concerns in key areas."	[none mentioned in guidance]

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			"Balancing the benefits and risks of AI, addressing biases and promoting equity among learners while protecting the data privacy of users is paramount to success when utilizing AI as a tool."	
Wyoming	-Data security -Data transfer -Data ownership -Data collection -Data storage -Data use	-Ensure AI system's compliance with data privacy and security policies -Vet AI systems for compliance with existing relevant laws -Scrutinize AI policies for how student data is used, stored, and collected	"When implementing AI systems, the key areas of technology policy to ensure compliance with are privacy, data security, student safety, data transfer and ownership, and child and youth protection. . . . Questions that need to be addressed include the following: ● What is the plan to conduct an inventory of systems and software to understand the current state of AI use and ensure adherence to existing security and privacy regulations? ● Does the education system enforce contracts with software providers, stipulating that any use of	SF 79 HB0008 HB0009

State	Privacy Considerations	Recommendations	Guidance Language	Referenced State Legislation
			AI within their software or third-party providers must be clearly revealed to district staff and first approved by district leadership? ● Does the plan take into account any implications for FERPA, CIPA, and COPPA, or if applicable, PPRA and GDPR?" "Review existing privacy policies that address student data. AI companies are not all educationally focused and how they collect, store, and utilize student data needs to be scrutinized. Privacy Policies may need to be examined to ensure that they cover AI"	