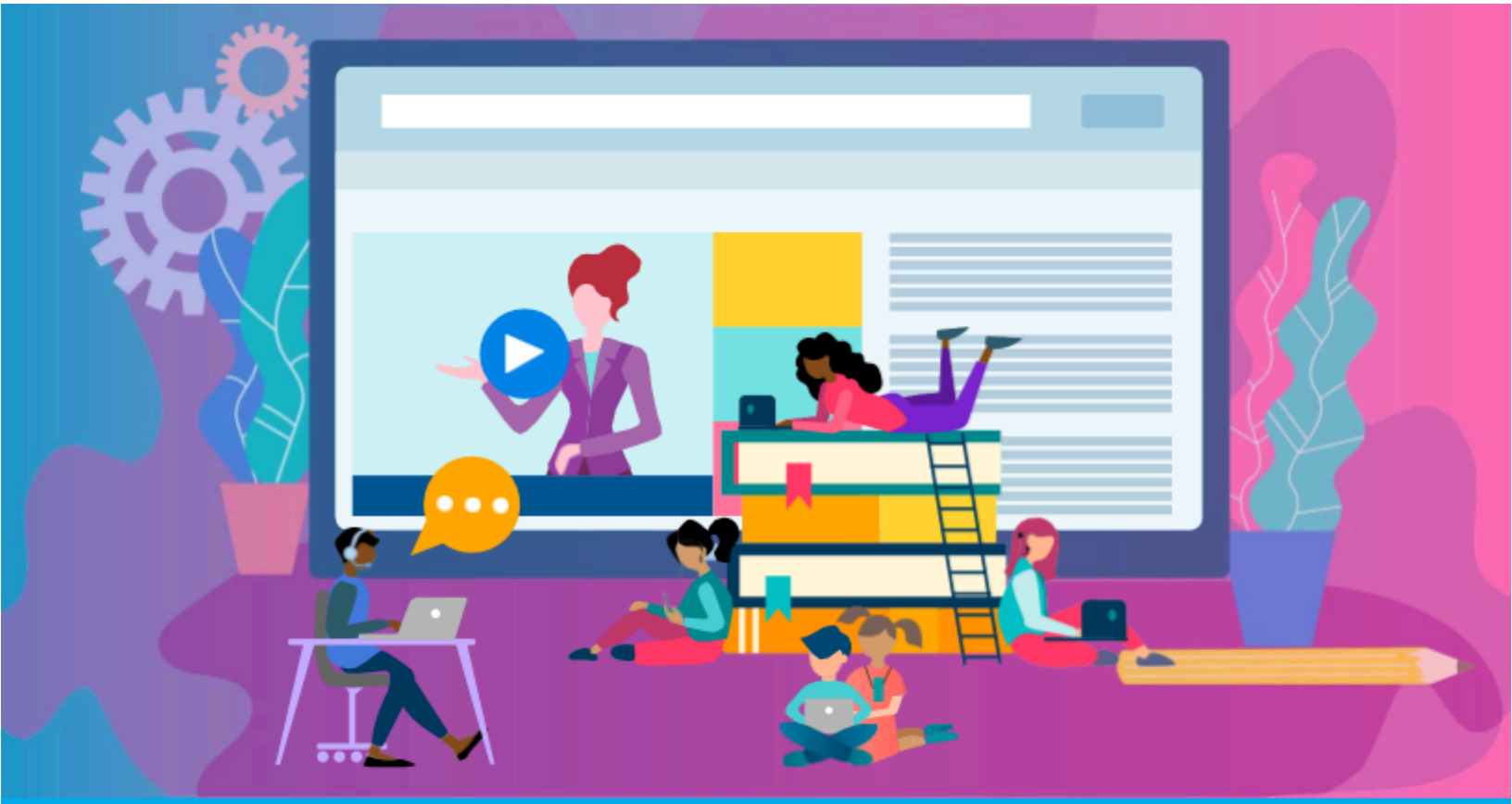
IT PASSES

An Education Technology Adoption Framework



June 2025

FUTURE OF PRIVACY FORUM

ABOUT THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a nonprofit organization focused on how emerging technologies affect consumer privacy. FPF is based in Washington, DC, and includes an advisory board comprised of leading figures from industry, academia, law, and advocacy groups.

FPF's Youth & Education Privacy program works to protect child and student privacy while allowing for data and technology use that can help young people learn, grow, develop, and succeed. FPF works with stakeholders from practitioners to policymakers, providing technical assistance, resources, trend analysis, and training.
FPF's Youth and Education Privacy team runs Student Privacy Compass, the one-stop-shop resource site on all things related to student privacy.

AUTHORS

Melissa Tebbenkamp, MSE, CETL
Technology Leadership and Privacy Consultant MBBT LLC

Jim Siegl, CIPT
Senior Technologist, Future of Privacy Forum

Erica Swanson, M.Ed
Consultant
Paritii

Amy Peterson, PhD
EdTech Practice Lead
Paritii

ACKNOWLEDGEMENTS

This publication builds upon the original IT PASSES concept developed and published by Jim Siegl under a Creative Commons (CC BY-NC 4.0) license in 2015. The current version incorporates adaptations and contributions by the Future of Privacy Forum.

:

Table of Contents

Executive Summary

The **IT PASSES** framework was developed to guide meaningful conversations around the safe development and adoption of K-12 online resources. It offers a structured approach to evaluating educational tools and platforms. It focuses on eight key areas critical to ensuring the responsible, effective, and sustainable use of technology with students. Each area is explored in its own section to provide deeper insight and practical considerations.The accompanying checklist is provided to assist online service providers in guiding collaborative discussions around the design and implementation of safe and effective digital solutions.

- **Interoperability**: Digital resources should integrate smoothly with existing district systems, including student information systems and learning management platforms. Interoperability enables seamless, secure, and controlled data exchanges, reducing administrative burdens, enhancing instructional continuity, and strengthening data privacy and security safeguards. Interoperability becomes increasingly more important with the integration of AI tools, and insufficient interoperability can limit AI's potential to provide insights, streamline processes, or reduce administrative burden.

- **Training**: Educators, students, and staff must receive timely, role-appropriate training to effectively use the technology. Ongoing professional development supports adoption, fidelity of use, and instructional impact. AI tools will fail to deliver their intended benefits if educators, students, and staff lack trust in the algorithms, the skills to use them fairly and effectively, and an understanding of their limitations.

- **Privacy**: Online tools must comply with applicable student data privacy laws (e.g., FERPA, PPRA, COPPA, and state regulations) and limit data collection to only what is necessary for educational use. Clear, transparent policies on data ownership, sharing, usage, retention, and third-party access are essential. In AI-powered learning environments, privacy protections and security must be considered in tandem with algorithmic accuracy driven by data availability and transparency. This is a balance that should be navigated with districts, educators, students, and families.

- **Accessibility**: Resources should be designed to meet the needs of all learners, including those with disabilities, following standards such as WCAG. Equitable access ensures every student can fully participate in digital learning. Designing, developing, and testing AI tools for users with a wide range of learning and accessibility needs can help ensure the tool is effective for all users.

- **Safety**: Digital environments must be designed to protect students from harmful content, interactions, and behaviors. Features like ensuring age-appropriate content, managing advertisements, providing moderation tools, controlled in-app communication, and offering clear reporting mechanisms contribute to safer user experiences. Systems that leverage AI must be tested thoroughly and continually iterated to mitigate the potential to generate or amplify harmful content, bias, or misinformation.

- **Security**: Robust cybersecurity measures should protect against unauthorized access, data breaches, and cyber threats. Key components include regular audits, encryption, secure and controlled data

transfers, and strong authentication protocols. Systems should also limit access to sensitive data based on user roles and maintain detailed audit logs to monitor and investigate activity. Data security becomes increasingly important when AI systems are implemented, as attackers can intentionally target the data or algorithms potentially impacting privacy, accuracy, and effectiveness.

- **Effectiveness:** Resources should demonstrate evidence of positive learning outcomes and support diverse student populations. Considerations should include cultural relevance, language accessibility, and support for varied learning styles. AI has the potential to impact student outcomes, but evidence may be limited on how adopting AI tools translates into meaningful learning outcomes for all students and justifies the investment of resources.

- **Sustainability/Scalability**: Solutions must be maintainable with available district resources and capable of scaling across schools or classrooms. Reliable support, clear documentation, and long-term viability are critical to success. In addition to a potential impact on infrastructure, sustainable AI tools must be adaptable as emerging technologies are implemented.

Introduction

The IT PASSES Framework

The IT PASSES Framework identifies eight critical focus areas that support the responsible, effective, and sustainable use of digital resources in K–12 education. Each framework component is further explored in its own standalone resource, providing deeper insight and practical considerations to guide meaningful conversations around the safe development and adoption of K-12 online resources. The accompanying checklist assists online service providers in guiding collaborative discussions around the design and implementation of safe and effective digital solutions.

- **Interoperability**: Digital resources should integrate smoothly with existing district systems, including student information systems and learning management platforms. Interoperability enables seamless, secure, and controlled data exchanges, reducing administrative burdens, enhancing instructional continuity, and strengthening data privacy and security safeguards. Interoperability becomes increasingly more important with the integration of AI tools, and insufficient interoperability can limit the potential of AI to provide insights, streamline processes, or reduce administrative burden.

- **Training**: Educators, students, and staff must receive timely, role-appropriate training to effectively use the technology. Ongoing professional development supports adoption, fidelity of use, and instructional impact. AI tools will fail to deliver their intended benefits if educators, students, and staff lack trust in the algorithms, the skills to use them fairly and effectively, and an understanding of their limitations.

- **Privacy**: Online tools must comply with applicable student data privacy laws (e.g., FERPA, PPRA, COPPA, and state regulations) and limit data collection to only what is necessary for educational use. Clear, transparent policies on data ownership, sharing, usage, retention, and third-party access are essential. In AI-powered learning environments, privacy protections and risk must be considered in tandem with security, algorithmic accuracy, and transparency, and this balance should be navigated with districts, educators, students, and families.

- **Accessibility**: Resources should be designed to meet the needs of all learners, including those with disabilities, following standards such as WCAG. Equitable access ensures every student can fully participate in digital learning. Designing, developing, and testing AI tools for users with a wide range of learning and accessibility needs can help ensure the tool is effective for all users.

- **Safety**: Digital environments must be designed to protect students from harmful content, interactions, and behaviors. Features like ensuring age-appropriate content, managing advertisements, providing moderation tools, controlled in-app communication, and offering clear reporting mechanisms contribute to safer user experiences. Systems that leverage AI must be tested thoroughly and continually iterated to mitigate the potential to generate or amplify harmful content, bias, or misinformation.

- **Security**: Robust cybersecurity measures should protect against unauthorized access, data breaches, and cyber threats. Key components include regular audits, encryption, secure and controlled data

transfers, and strong authentication protocols. Systems should also limit access to sensitive data based on user roles and maintain detailed audit logs to monitor and investigate activity. Data security becomes increasingly important when AI systems are implemented as these systems have been intentionally targeted and could have additional vulnerabilities.

- **Effectiveness:** Resources should demonstrate evidence of positive learning outcomes and support diverse student populations. Considerations should include cultural relevance, language accessibility, and support for varied learning styles. AI has the potential to impact student outcomes, but evidence may be limited on how the adoption of AI tools translates into meaningful learning gains for all students and justifies the investment of resources.

- **Sustainability/Scalability**: Solutions must be maintainable with available district resources and capable of scaling across schools or classrooms. Reliable support, clear documentation, and long-term viability are critical to success. In addition to a potential impact on infrastructure, sustainable AI tools must be adaptable as emerging technologies are implemented.

Connections Across the IT PASSES Framework

Each component of the IT PASSES Framework is interconnected, with overlapping considerations that reinforce one another. For example, privacy and security are closely related but distinct concepts in the management of student data. Privacy refers to how information is collected, used, and shared. Security encompasses the technical and administrative safeguards that protect data from unauthorized access, breaches, or misuse. Within the scope of privacy, additional attention is given to confidentiality and compliance. Confidentiality involves the ethical and professional responsibility to prevent the unauthorized disclosure of sensitive information. Compliance involves adhering to applicable laws, regulations, and policies such as FERPA, COPPA, or state-level statutes that govern the appropriate handling of student data. While privacy represents the intended outcome, security and confidentiality are the mechanisms that protect it, and compliance ensures these practices are aligned with legal and regulatory standards.

Interoperability

Interoperability ensures that digital resources can integrate efficiently with a district's existing technology ecosystem, including student information systems (SIS), learning management systems (LMS), assessment platforms, data dashboards, and other instructional tools. When systems communicate seamlessly, districts can reduce data silos, streamline workflows, enhance instructional continuity, and reinforce privacy and security through controlled data exchange. Interoperability has become increasingly more important with the integration of AI tools.

Why it Matters

Without thoughtful design and implementation, poor interoperability can introduce significant risks to student data privacy, operational effectiveness, and instructional reliability.

- Systems that do not allow districts to control which data fields are shared or lack data minimization features may result in unnecessary exposure of sensitive student information.
- Inadequate access controls between systems can lead to unauthorized data access or inconsistent application of user roles.
- Misalignment of data caused by improper field mapping, outdated or unsupported standards, or lack of data validation can undermine reporting accuracy and hinder decision-making.
- Manual workarounds such as file uploads or spreadsheets increase the risk of human error and data breaches, while rigid systems that limit integration options can constrain innovation and district flexibility.
- Insufficient interoperability can limit the potential of AI to provide insights
- Fragmented and siloed data can hinder efforts to identify and address disparities in resource allocation, support services, and interventions across all student groups.
- The lack of systems integration could disproportionately impact educators who serve student populations with a wide range of specific learning needs (English language learners, students with exceptionalities, students who need additional behavioral support, etc.) as they may already spend more time coordinating various support services and accommodations.

Practical Implementation Strategies

Districts, educators, and students benefit from streamlined interoperability, freeing up precious time so educators can focus on effective instruction. To maximize the benefits and reduce the risks, interoperability must be prioritized as a foundational element of any digital learning strategy.

- ☐ Build and maintain products using open interoperability standards to reduce barriers to adoption.
  - ☐ Adopt an industry-recognized data standard such as OneRoster, Learning Tools Interoperability (LTI), and Ed-Fi to facilitate system-to-system integration. Clearly identify the standard used.
  - ☐ Provide clear documentation detailing alignment with the selected interoperability standard, including version, field mapping, required vs optional fields, data types, payload structure, authentication methods, and any deviations from the standard implementation.
  - ☐ Provide clear technical documentation and dedicated support for integration planning and troubleshooting.
  - ☐ Implement a procedure to continually validate that data formats are compliant with standard definitions.
- ☐ Conduct a system integration audit to identify key platforms and their data dependencies before onboarding new districts.
- ☐ Use API-based connectors or middleware to streamline data sharing and reduce the need for manual data entry.

- [ ] Implement data minimization protocols when configuring integrations to share only the specific data fields required for the tool's operation.
  - [ ] Limit required fields to those necessary for core functionality, allowing the remaining data points to be optional.
  - [ ] Enable districts to control data flow, including selective data field syncing and role-based permissions, to support local governance needs.
- [ ] Require data mapping validation during implementation to ensure fields are aligned correctly across platforms, reducing errors and reporting inconsistencies.
- [ ] Establish clear governance policies for how data is shared across systems, ensuring access is secure, purposeful, and role-based.
- [ ] Prioritize tools that support automated rostering, single sign-on (SSO), and real-time updates to reduce administrative load and improve user experience.
- [ ] Demonstrate interoperability as part of product demos, pilots, and procurement processes.

AI Considerations

Interoperability becomes increasingly more important with the integration of AI tools. Insufficient interoperability can limit the potential of AI to provide insights, streamline processes, or reduce administrative burden.

- Implement data minimization protocols and enable districts to control the use and sharing of sensitive data in AI systems.
- Create data maps and validation requirements to mitigate the risk of inaccurate or incomplete data being fed into AI, which can amplify existing biases in the data and lead to inaccurate AI-driven recommendations or assessments.
- Consider how interoperability, authentication systems, and ease of rostering can lead to unintended leaks of personal data into AI systems

Questions districts may ask

- Does the solution support integration with our core systems (SIS, LMS, identity provider, etc.)?
- Can you provide documentation of supported standards (e.g., OneRoster, LTI) and evidence of successful integrations in similar environments?
- What are your practices around data access and retention? What safeguards do you have in place?

Framework Connections

Interoperability and Accessibility

Gaps in interoperability can introduce accessibility barriers if the integration does not fully support or pass through accessibility-related metadata or settings. For example, a service provider may design their tool to meet WCAG 2.1 AA standards, but when integrated with a third-party system, the systems fail to appropriate map or communicate user preferences such as high-contrast mode, text resizing, or screen reader settings. As a result, students who rely on these settings experience a degraded or inaccessible experience when accessing the tool.

Interoperability, Data Privacy and Security

Interoperability, data privacy, and security are tightly connected components within the IT PASSES Framework, especially in environments that rely on automated data exchange and single sign-on (SSO) systems. Seamless integration between systems such as through rostering tools or SSO platforms like “Sign in with Google” can streamline access and reduce administrative overhead, but also introduces privacy and security risks if not carefully managed. When interoperability is not implemented with strong controls, there is an increased risk of data leakage, where unnecessary or excessive personal data is shared across systems without clear purpose or oversight. Similarly, unapproved data sharing can occur if districts are unable to restrict which fields are transmitted during integration or if third-party platforms access data beyond what is educationally necessary. Inadequate security configurations in SSO or rostering setups can also expose sensitive student information during transmission or authentication.

Training

Effective use of digital resources depends on more than just access to technology—it requires timely, relevant, and role-specific training for educators, students, and support staff. High-quality training ensures that users not only understand how to operate the tools, but also how to integrate them into teaching, learning, and daily workflows in meaningful ways. When professional development is thoughtfully planned and embedded throughout the lifecycle of a digital resource, it increases user confidence, strengthens instructional impact, and improves fidelity of use.

The success of AI tools is dependent on educators, students, and staff trusting the algorithms and having the skills necessary to use them fairly and effectively, including an understanding of their limitations.

Why it Matters

Insufficient or generic training can lead to inconsistent implementation, underutilization of selected tools, and frustration among educators and students.

- Without training tailored to specific user roles, such as instructional staff, administrators, and technology support staff, users may miss critical functionality or apply tools ineffectively.

- A lack of ongoing or just-in-time support can result in reduced engagement over time, even when platforms have strong instructional potential.
- Without usage insights to identify training gaps, districts may stop investing in tools that are not being fully adopted or understood instead of providing the additional training.
- AI tools will fail to deliver their intended benefits if educators, students, and staff lack trust in the algorithms, the skills to use them fairly and effectively, and an understanding of their limitations.

Practical Implementation Strategies

To build long-term value and positive learning outcomes, training must be seen as a continuous, data-informed process.

- ☐ Provide clear documentation, training materials, and helpdesk support as part of procurement and onboarding.
  - ☐ Develop onboarding resources for each user group, including teachers, administrators, students, and support staff.
- ☐ Build time for training into suggested implementation schedules.
  - ☐ Provide onboarding toolkits and orientation resources that schools can deploy independently.
- ☐ Ensure training is differentiated by role and aligned with users' responsibilities and addresses varied technical proficiency levels.
  - ☐ Design and deliver training that is flexible, modular, and tailored to a variety of user roles and learning preferences.
  - ☐ Provide access to just-in-time resources that are geared towards different learning styles such as searchable help centers, video tutorials, and step-by-step guides.
- ☐ Align training with product updates and release cycles to keep users informed of new features and best practices.
  - ☐ Maintain up-to-date knowledge bases, FAQs, and video libraries for on-demand support.
- ☐ Offer ongoing professional development opportunities, including train-the-trainer models, webinars, and asynchronous modules.
- ☐ Collect and analyze usage data to identify training gaps and target areas for support.
  - ☐ Partner with districts to analyze usage data and recommend training paths that close identified gaps.

AI Considerations

It is essential to consider the broader context of the technology when designing a training plan. When introducing AI technologies, training should extend beyond the tool itself to support educators, students, and families in better understanding how AI utilizes data to create recommendations and content.

- Provide clear documentation regarding data utilization and AI decision-making and its limitations
- Develop plans to assess and address AI literacy
- Create specific AI tool training for school systems addressing the unique contexts of the solution
- Develop or utilize existing AI literacy training tools to support broader AI understanding, transparency, and user autonomy

Detailed resources on AI literacy, education, and awareness-building are provided in the Responsible AI Guide: https://www.paritii.com/detail/ai-literacy-education-awareness-building

Questions districts may ask

- How does the platform include differentiated training aligned to staff roles and district goals?
- Is professional development ongoing or one-time?
    - Is the professional development offered in-person, virtual, and/or self-paced?
- What usage or adoption analytics are available to support targeted follow-up training?
- How does your provided training support both instructional use and back-end configuration, especially for instructional technology and technology support staff?
- What information do you provide to assist us in training our staff on decision making when using your AI tools?

Framework Connections

Training and Effectiveness

Staff and student training, or lack thereof, directly impacts the effective use of digital resources and student outcomes. System effectiveness requires timely, relevant, and role-specific training for educators, students, and support staff.

Training, Privacy, Safety and Security

AI literacy training supports users in effectively advocating for their privacy, safety, and security needs and improves transparency.

Privacy

Protecting student data privacy is both a legal obligation and an ethical imperative for schools. Online service providers must ensure compliance with the Children's Online Privacy Protection Act (COPPA) and online tools must enable districts to comply with applicable privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). States may also have additional privacy regulations. Beyond compliance, service providers and districts must work collaboratively to ensure that data practices prioritize data privacy and security, student safety, educational necessity, and transparency.

Why it Matters

When privacy is not thoughtfully addressed, there is a risk exposing sensitive student information, violating legal requirements, and eroding trust.

- Systems that collect more data than necessary or do not clearly define ownership and access can create serious data privacy concerns.
- Vague or overly broad privacy policies may allow for undisclosed data sharing with third parties or unapproved uses of identifiable information.
- Without safeguards to review and control how data is used, particularly when new features are introduced, products may fall out of alignment with established privacy practices.

Practical Implementation Strategies

Strong data privacy requires continuous oversight, clear communication, and a commitment to minimizing data use. Both school districts and service providers must engage in regular dialogue to ensure that privacy policies are meaningful, enforceable, and responsive to evolving technologies and legal standards.

- Develop and maintain privacy policies and terms of service that are easy to understand, transparent, and tailored to K–12 education.
- Limit data collection to what is essential for educational functionality and clearly document how it is used.
- Ensure data ownership, access rights, and retention policies are explicitly defined and accessible in policy or support documents.
- Verify that all third-party data sharing practices are fully disclosed and limited to educational purposes.
- Implement review protocols for any new system features that modify how data is collected, accessed, or shared.

- Create a feedback loop to allow districts to weigh in on changes that affect data use or privacy.
- Build privacy checkpoints into product update cycles and change management workflows.
- Ensure alignment with contractual privacy agreements throughout the product lifecycle.
- Clearly define and enforce student data retention schedules that align with legal requirements, ensuring data is deleted or anonymized when no longer needed for educational purposes.
    - Support district-specific retention preferences, including early deletion or data export.
    - Ensure secure data deletion or anonymization once no longer needed, upon district request, or when the contract is terminated or non-renewed.

AI Considerations

There is a delicate balance that must be navigated with privacy protections when implementing AI. Large datasets with comprehensive data can improve AI accuracy; however, this can also undermine the need to collect and use only the most necessary data to protect privacy. Developers must adopt responsible AI development practices to protect student privacy and mitigate potential harm. The tradeoff between privacy and accuracy should be carefully considered and addressed transparently with school districts, school leaders, and families.

- Utilize an AI nutrition Label to build trust in your product.
- Limit data collection in AI-driven systems.
- Establish guardrails to ensure identifiable data is not unintentionally disclosed in generative AI responses.
- When possible, de-identify data and remove sensitive variables when developing algorithms for AI tools.
- Provide transparent documentation of pre-sanitization protocols that include and prioritize privacy safeguards, bias identification, and mitigation.
- Provide transparent documentation of data removal protocols that include the impact analysis on model performance, data representativeness, and potential for introducing or exacerbating bias.
- Provide transparent documentation of proxying techniques in use, the rationale for use, the potential limitations, and the risks associated with the technique for the specific context.

A comprehensive guide on responsible AI development in EdTech can be referenced here: https://www.paritii.com/detail/data-methodology

Questions districts may ask

- How does the privacy policy and terms of service reflect educational-specific needs and comply with federal and state laws and district requirements?
- What data minimization principles are applied to ensure that only necessary data is being collected?
- Does your system have the ability for the district to configure or restrict data sharing settings based on district policy?
- What is your communication process for product updates that include changes to data use? Do you provide advance notice of new features that impact privacy?
- Do you have documented student data retention policies in accordance with federal, state, and local requirements? What are your data retention practices?
- How do you ensure the deletion or anonymization of student data once it is no longer necessary for educational use or after contract termination?
- What documentation do you provide for the pre-sanitization, removal, and proxying of data?

Framework Connections

Privacy, Security, and Interoperability

In AI-powered learning environments, privacy protections and risk must be considered in tandem with interoperability and security. Without clear policies and technical safeguards in place, there is a heightened risk of data overexposure, where student information that is not essential for educational use is unnecessarily shared across integrated systems. Privacy concerns may also arise when districts are unable to control which data fields are transmitted or lack visibility into how third-party systems access and use student information. Inadequate security configurations within SSO or rostering tools can further compromise privacy by exposing sensitive information during transmission or user authentication.

Privacy and Effectiveness

Transparency is a fundamental component of student data privacy. As digital tools increasingly incorporate artificial intelligence, service providers must ensure that school districts understand how student data is used, particularly in automated decision-making processes. A lack of clarity regarding how data is collected, analyzed, or shared can obscure the presence of bias or result in privacy violations that districts are not able to detect or prevent. To support privacy protections, service providers must clearly document data flows, provide meaningful explanations of AI-driven features, and ensure that schools retain oversight of how student data is used. This balance between innovation and transparency is essential to maintaining compliance, trust, and ethical data use.

Accessibility

Digital learning environments must be inclusive and accessible to all students, regardless of ability. This includes designing educational tools and platforms in alignment with recognized accessibility standards such as the Web Content Accessibility Guidelines (WCAG) 2.1 AA and Section 508 of the Rehabilitation Act. When accessibility is prioritized, students who rely on assistive technologies such as screen readers, captioning tools, or alternative input devices can fully participate in learning alongside their peers.

Why it Matters

Failure to meet accessibility standards can create barriers for students with disabilities, limit equitable learning opportunities, and put schools at risk of noncompliance with federal laws.

- Inaccessible content or poor navigation design can reduce engagement, hinder comprehension, and exclude learners from classroom activities or assessments.
- Inconsistent support for assistive technologies or a lack of flexibility in visual customization can make digital tools unusable for some students.
- Ensuring accessibility requires routine evaluation, user feedback, and an ongoing commitment to inclusive design.

Practical Implementation Strategies

Equity in access is foundational to student success. School districts and service providers must work together to ensure that all students can engage with digital content in ways that meet their diverse needs and support their right to a high-quality, inclusive education.

- Design products with accessibility as a core principle from initial development through ongoing updates.
    - Ensure all product offerings demonstrate conformance with WCAG 2.1 AA and Section 508 standards.
    - Conduct internal testing and third-party audits during the development process and at regular intervals post-release to validate accessibility compliance.
    - Document how accessibility is tested and maintained throughout product development.
- Maintain up-to-date documentation on accessibility features, compatibility, and known limitations.
- Clearly disclose which assistive technologies are supported and provide guidance on optimal configurations.
- Ensure compatibility with widely used assistive technologies (e.g., screen readers, voice input, closed captioning, keyboard navigation).

- Provide options for customizing visual display, such as text resizing, color contrast, and alternative text for images.
- Include accessibility review as part of the instructional design processes.
    - Involve students with disabilities and accessibility experts in usability testing and feedback loops.
- Ensure reliable, responsive reporting mechanisms for any accessibility-related issues or feature limitations.
    - Engage with districts to address accessibility concerns proactively and respond to feedback from users with diverse needs.

AI Considerations

If the data used to train AI models lacks representation from individuals with disabilities or if the development team lacks awareness of accessibility needs, the resulting AI tools might inadvertently perpetuate existing biases and create new accessibility barriers. Designing, developing, and testing the AI tool with users who have a wide range of learning and accessibility needs can help ensure the tool is effective for all users.

- Ensure training data includes individuals from diverse backgrounds and individuals with disabilities or unique learning needs
- Involve individuals from different backgrounds in the design and development process
- Provide transparent documentation and explanations for how the AI tool adapts content and interfaces for user disabilities and offers customization options where appropriate
- Establish a routine audit process for AI-generated content and recommendations for accessibility and bias to ensure the tool continues to address the specific needs of all learners, particularly as AI capabilities evolve and functionalities are added

Questions districts may ask

- How do you ensure product alignment with WCAG and Section 508 standards?
- Do you have accessibility conformance reports (e.g., VPAT)?
- Which assistive technologies are or are not supported?
- How do your platforms support inclusive navigation and customizable visual settings for a range of learners?
- How do you ensure accessibility features remain intact through updates and feature changes?

Framework Connections

Accessibility, Interoperability and Effectiveness

Accessibility, interoperability, and effectiveness are interdependent elements that online service providers must consider when designing and delivering digital resources. A product may be instructionally effective and aligned with academic standards, but if it does not meet accessibility requirements or fails to integrate with district systems, its value to schools is significantly reduced. Interoperability must support the transfer and preservation of accessibility settings and assistive technology compatibility across platforms to ensure a consistent user experience for all students. Additionally, accessibility features such as customizable display options, keyboard navigation, and screen reader support directly contribute to broader instructional effectiveness by addressing diverse learning needs. To maximize impact and adoption, service providers should approach product development with a holistic focus that aligns accessibility, interoperability, and learning outcomes.

Safety

Creating a safe digital space is essential to supporting student well-being and maintaining a productive learning environment. Online resources must be intentionally designed to protect students from harmful content, inappropriate interactions, and unsafe online behaviors. As students increasingly engage with digital tools for learning, communication, and collaboration, platforms must include safeguards that ensure age-appropriate content, manage exposure to advertisements, and regulate communication features. Online tools used in the K–12 environment should incorporate built-in safeguards such as age-based content filtering, advertisement management, communication controls, and reporting mechanisms. Effective safety measures not only protect students but also build trust with families and educators.

Why it Matters

Without embedded safety controls, online platforms can expose students to inappropriate media, unmoderated peer interactions, or even external threats.

- Failure to differentiate features based on student age or role increases the likelihood of misuse or harm, particularly when in-app communication tools are unregulated.
- The presence of advertising in student-facing environments can introduce ethical and developmental concerns, especially if ad content is not screened or restricted.
- Unclear or unavailable reporting tools and response protocols may cause incidents to go unaddressed, leaving students vulnerable and undermining a district's responsibility to provide a safe learning environment.

Practical Implementation Strategies

Ensuring student safety requires thoughtful collaboration between school districts and service providers. Together, they must implement safeguards that are adaptable to various age groups, configurable at the district level, and aligned with both educational and community expectations.

- ☐ Prioritize age-appropriate content delivery across all product features.
  - ☐ Eliminate advertisements when possible; at a minimum, ensure they are fully controlled and age-appropriate in student-facing areas.
- ☐ Design systems that distinguish user roles and implement safety measures tailored to student age and context.
  - ☐ Align in-app communications with user roles and ensure safeguards are in place for younger learners.
- ☐ Configure communication tools to allow district-level control based on student age, role, or instructional context.
- ☐ Incorporate filtering, moderation, and flagging tools to detect and respond to inappropriate content or behavior.
- ☐ Include accessible and actionable reporting mechanisms for inappropriate content or behavior that are visible and easy to use for students and staff.
- ☐ Offer visibility and control to administrators over interactions, user-generated content, and real-time activity monitoring.
- ☐ Collaborate with districts to share digital safety guidance and clearly document response protocols for unsafe interactions.

AI Considerations

In addition to unsafe and potentially harmful content, AI can produce inaccurate, inappropriate, or biased content when left unchecked. While LLMs typically perform well on knowledge-based prompts, they are less effective with reasoning and can often produce biased content. The performance of these models varies, leaving room for developers to select models that have a lower risk of exposing students to potentially inaccurate or harmful content and spreading misinformation.

AI models employed for predictive analytics, early alerts, interventors, or other use cases that may influence decision-making can potentially expose students to harm. For example, if an algorithm is less effective at accurately identifying students in particular demographic groups as ‘at-risk’, it could suggest interventions that negatively impact the student’s learning progress. Transparency about the risks and limitations of the AI algorithm is essential to help school leaders and users contextualize the recommendations and make decisions that are in the student's best interest.

- Implement continuous monitoring protocols to mitigate the potential for harm. These should be both transparent and involve the input of districts, school leaders, and other impacted parties.

- If leveraging LLMs for AI-enabled features, use bias audits and benchmarks to understand the potential to introduce harmful, inaccurate, and biased content
- Implement continuous monitoring protocols to evaluate how the algorithm is responding to prompts and make adjustments
- Provide transparent documentation about bias mitigation techniques employed and algorithmic limitations
- Identify proxy variables that may lead to the categorization of data based on patterns that result from systemic bias with intention to reduce the risk of decisions made utilizing such algorithms

Questions districts may ask

- Do you offer and support customizable safety settings that can be aligned with district policy and student developmental levels?
- Are age-based controls available for communication, content access, and interaction features?
- How are advertisements handled? Are they removed in student environments?
- What moderation tools and reporting dashboards are available? What is the process and support expectations for handling incidents?
- What training and resources are available to educators and families to help them understand safety features and usage guidelines?
- What continuous monitoring protocols are in place to evaluate potentially harmful, unsafe, inaccurate, or inappropriate content?

Framework Connections

Safety, Privacy and Security

Safety, privacy, and security are interconnected priorities that must be addressed collectively in the design and delivery of digital tools for K–12 education. While privacy focuses on the appropriate collection, use, and sharing of student data, and security provides the technical safeguards that protect that data from unauthorized access, safety ensures that students are protected from harmful content, interactions, and behaviors while using the platform. A weakness in one area can compromise the effectiveness of the others. For example, insufficient content moderation or unregulated communication features may expose students to unsafe situations, while weak access controls or poor data governance can lead to unauthorized sharing of personal information. Online service providers must ensure that safety features are not implemented in isolation, but are supported by secure infrastructure and privacy-centered data practices that align with legal requirements and community expectations.

Security

Strong cybersecurity practices are essential to protecting sensitive student data, ensuring system reliability, and maintaining the integrity of digital learning environments. Online educational tools must be built with safeguards that prevent unauthorized access, mitigate cyber threats, and support secure operations across all user groups. Effective security practices include regular system audits, encryption protocols, secure data transfers, role-based access controls, and detailed activity logging.

Why it Matters

When cybersecurity is not prioritized, districts may face serious consequences, including data breaches, system downtime, and violations of privacy laws.

- The lack of encryption or secure authentication methods can expose student information to external threats.
- Unclear access permissions or the absence of audit logs can make it challenging to detect misuse or respond effectively to security incidents.
- Without proactive security assessments and alignment with recognized standards, online tools may fall short of meeting the security expectations of K–12 schools.
- Data breaches could disproportionately harm certain students based on the sensitivity of their information (special education records, disciplinary actions, health information, details indicating socioeconomic status, family living situation, etc.)

Practical Implementation Strategies

Data security is a shared responsibility between school districts and service providers. Ongoing collaboration and transparent communication are necessary to ensure that digital learning environments remain secure, resilient, and responsive to emerging threats.

- ☐ Protect all sensitive data using encryption standards that meet or exceed industry best practices.
  - ☐ Use secure data transfer protocols for both API-based integrations and other forms of data exchange.
  - ☐ Ensure the encryption of data both in transit and at rest, and confirm the scope and strength of the encryption methods used.
- ☐ Support secure and flexible authentication methods and provide clear integration options for district identity systems.
  - ☐ Implement secure authentication methods, such as single sign-on (SSO) and multi-factor authentication (MFA), where applicable.
- ☐ Configure access based on user roles and responsibilities, ensuring that users can only access the data required for their function.
- ☐ Maintain detailed audit logs that track system activity, including login events, data access, and administrative changes and make summaries available to districts upon request.
- ☐ Establish retention timelines and access controls for audit logs to support incident investigation and compliance requirements.

- [ ] Conduct regular internal and third-party security assessments to identify vulnerabilities and verify the effectiveness of existing controls.
- [ ] Align system design and practices with established cybersecurity frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or Center for Internet Security (CIS) Controls.
- [ ] Develop clear, documented incident response and breach notification protocols that define expectations for communication with districts and procedures for handling security incidents as part of contractual agreements.
- [ ] Implement data lifecycle management practices that include routine review and secure deletion of student data according to retention policies, minimizing the risk of unnecessary data exposure or misuse.
    - [ ] Provide districts with clear control over data retention settings and the ability to request deletion at any time.
    - [ ] Conduct periodic reviews of stored data to ensure it is retained only as long as necessary for agreed-upon educational purposes.

AI Considerations

Ineffective cybersecurity measures could expose schools to risks like data poisoning and adversarial attacks. Data poisoning refers to injecting biased or corrupted data into the training process to manipulate the AI's behavior. This can impact recommendations, lead to unfair assessments, or generate harmful content.

- Develop transparent documentation on the training data pipeline and measures to protect against data poisoning.
- Protect against user initiated adversarial attacks designed to manipulate the algorithm itself. For example, users may be able to bypass content filters or influence AI-powered grading systems.
- Develop transparent documentation for districts, school leaders, and families about the risks and safeguards in place to mitigate data poisoning, adversarial attacks, and other security threats specific to AI technologies.

Questions districts may ask

- Do you encrypt data both in transit and at rest? What technical methods are used?
- What user authentication options are available?
- How are user roles defined? How is access to data restricted to roles managed by the district?
- Can you provide documentation on audit logging, including the types of activities tracked and log retention practices?
- What are the established protocols for incident response and breach notification?

- What are your data deletion procedures and how can we assure they align with district data retention policies?
- Are student data retention and deletion requirements defined in the data sharing agreement?

Framework Connections

Security and Privacy

Online service providers must balance the need for strong security protections with the transparency required by school districts to manage risk effectively. In environments that use artificial intelligence or other automated processes, the lack of visibility into how systems operate, often referred to as the "black box" problem, can pose challenges for detecting security vulnerabilities, managing access controls, or responding to incidents. When school systems are unable to fully understand or audit how information is processed or protected, it can lead to gaps in oversight and reduce trust in the product. Service providers should ensure that even in security-sensitive contexts, transparency regarding data handling, authentication processes, and risk mitigation strategies is provided to school and district leaders

Effectiveness

Educational technology should contribute meaningfully to student learning and serve the diverse needs of all learners. Digital resources should be grounded in sound instructional design and supported by evidence that demonstrates their positive impact on student achievement. To be truly effective, tools must also reflect a commitment to equity by accommodating varied learning styles, addressing language needs, and offering culturally relevant content.

Why it Matters

When tools are selected without consideration for their instructional value or adaptability, districts may invest in platforms that are underutilized or misaligned with learning goals.

- Tools that do not reflect the diversity of the student population or support inclusive teaching practices can create gaps in engagement and outcomes.
- A lack of data on usage, fidelity of implementation, or student outcomes makes it difficult to determine whether a resource is having its intended effect.

Practical Implementation Strategies

Ensuring that educational tools are effective for all learners requires shared responsibility between school districts and service providers. Together, they must prioritize instructional relevance, cultural responsiveness, and ongoing evaluation to support student growth across all learning environments.

- ☐ Provide evidence of educational effectiveness through research, case studies, or pilot results.
- ☐ Design content and features that support a broad range of learners, including those with different cognitive, linguistic, and cultural needs.
  - ☐ Ensure tools support a range of instructional approaches, including differentiated instruction, scaffolding, and student self-pacing.
  - ☐ Offer multilingual content and ensure cultural responsiveness in both curriculum and platform design.
- ☐ Include educators and curriculum leaders in the design process to ensure alignment with practitioner priorities.
- ☐ Utilize Universal Design for Learning (UDL) principles and accessibility for various learning profiles.
- ☐ Enable districts to monitor usage patterns and student progress through dashboards and exportable reports.
  - ☐ Include evaluation metrics and impact reports to support evidence-based decision-making.
- ☐ Regularly collect user feedback from students and educators to refine use and identify gaps in effectiveness or inclusivity.

AI Considerations

Some AI technologies are less accurate for specific demographic groups, which introduces a significant risk to effectiveness for all students. Districts, school leaders, and educators make critical decisions based on the output of AI technologies so it is essential that they understand the algorithms they are working with and their limitations. In designing products to meet the needs of K12 schools, service providers should consider some of the common challenges and incorporate bias mitigation strategies in their development processes.

- Ensure training data is reflective of the demographics of the school population to prevent historical data trends from inadvertently perpetuating existing bias
- Identify proxy variables that may lead to the categorization of data based on patterns that result from systemic bias in order to mitigate the potential harms from using recommendations based on that data
- Plan for a robust testing and iteration process to identify populations and subgroups for which the algorithm is less accurate
- Clearly communicate the documented risks and biases found in similar technologies and the steps you have taken to mitigate them
- Develop bias monitoring protocols to ensure that the AI algorithm is accurate for and effective across all student demographic, socioeconomic, and ability groups
- Define the appropriate use of the outputs of AI algorithms to avoid unintended use, for example, using engagement tracking for grading purposes rather than as an instructional tool

More context and guidance on how to promote responsible AI is available here: https://www.paritii.com/detail/why-equitable-ai

Questions districts may ask

- What documentation or research exists to support the product's claims of instructional effectiveness?
- How does the tool support multiple learning styles and instructional strategies?
- How does the content reflect the cultural, linguistic, and socio-economic diversity of our student population?
- What usage or outcomes data is available to monitor implementation success?
- How do you involve instructional leaders and classroom educators in evaluating ongoing impact and instructional alignment?

Framework Connections

Effectiveness and Privacy

Effectiveness must be evaluated not only by instructional outcomes but also by how responsibly student data is used to support those outcomes. When digital tools rely on student information to personalize learning, generate reports, or conduct internal research, it is essential that data use remains limited, transparent, and aligned with legal requirements. Service providers must clearly articulate how student data contributes to educational effectiveness and ensure that all data practices are disclosed in a way

that supports informed district oversight. Using student data for research, even with the intent of product improvement, requires special consideration. Providers must avoid using identifiable student information without appropriate consent and must be prepared to demonstrate how research activities comply with applicable privacy laws and ethical standards.

Sustainability and Scalability

The long-term success of any digital resource is dependent on its maintainability and adaptability over time. Solutions must be scalable to meet the needs of classrooms, schools, and entire districts while remaining sustainable within the limits of district capacity and resources. This includes providing reliable technical support, accessible documentation, cross-platform compatibility, and a clear product roadmap that demonstrates a commitment to ongoing relevance and performance.

Why it Matters

When tools are difficult to scale or lack adequate support, districts may face inconsistent implementation, increased demands on technology support staff, or early abandonment of the product.

- A lack of transparency around update schedules, patching practices, or long-term development goals can erode confidence in the tool and create operational inefficiencies.
- Insufficient training or guidance can lead to uneven use across classrooms and reduced impact on student learning.

Practical Implementation Strategies

To ensure both supportability and scalability, school districts and service providers must work together to establish shared expectations around technical support, growth planning, and continuous improvement. A focus on long-term partnership and product evolution helps ensure that digital resources remain viable and effective over time.

- Ensure compatibility across commonly used devices, operating systems, and browsers in K–12 schools.
- Provide clear and comprehensive documentation for installation, configuration, usage, and troubleshooting.
- Establish direct channels for timely and effective technical support, including service level expectations.
- Provide implementation support and training to help districts deploy the solution consistently and effectively.
- Develop scalable deployment models that support transitions from pilots to full-scale rollouts.
- Communicate system updates, patches, and known issues in a timely and accessible manner.
- Release product updates and security patches on a consistent schedule and maintain public changelogs.
- Share a product roadmap that includes future enhancements and demonstrates long-term viability.

- Incorporate user feedback into product development to ensure relevance and responsiveness to district needs.

AI Considerations

AI applications often require significant computational resources, storage, and network bandwidth. Cloud-based AI solutions can offer scalability by leveraging remote infrastructure, potentially reducing the burden on local district resources; however, this requires consistent connectivity.

- Conduct a readiness assessment before implementing AI solutions to ensure adequate computational resources, storage and bandwidth
- Design tools and roadmaps that are adaptable in the integration of emerging technologies.
- Determine how generative AI tools will be trained and the role student data will play in training the model.

Questions districts may ask

- What technical and human resources are needed in the district to ensure the product is effectively supported?
- What technical support do you provide? How is it structured?
- What documentation do you provide and how do you review it for clarity, completeness, and accessibility for various staff roles?
- How do we scale the implementation from limited use (e.g., pilot) to district-wide adoption without requiring significant reconfiguration?
- How are updates communicated and do they align with change management processes?
- What fiscal and human resources are necessary for the implementation and sustainability of the product?

Framework Connections

Sustainability, Scalability, and Security

Sustainability and scalability play a critical role in maintaining a secure digital learning environment. As products expand across classrooms or districts, service providers must ensure that security controls scale appropriately with usage. A lack of routine updates, delayed patching, or outdated security protocols can introduce vulnerabilities that put student data at risk. To reduce risk, online service providers should implement regular security assessments, ensure timely distribution of patches, and maintain transparency with school systems about product development and end-of-life timelines.

Sustainability, Scalability, Training and Effectiveness

A tool's instructional effectiveness can only be sustained if the product remains usable, well-supported, and adaptable over time. When digital resources cannot scale effectively, lack ongoing support, or are not used with fidelity, their educational value declines as implementation becomes inconsistent or outdated. Instructional features that are not properly utilized, maintained or aligned with evolving classroom needs may limit engagement, reduce impact, or lead to abandonment.

Conversation Guide

** Indicates an AI focused discussion*

Interoperability

- Does the product support standard data formats (e.g., OneRoster, LTI, Ed-Fi)? If so, which formats/versions? How do you ensure the product stays current with the selected standards?
    - What API or connectors are available for customized integration? Are these publicly available or at a minimum available for developers? How is the API supported and is there an additional cost?
- What systems does the product integrate with and is the integration natively supported or does it require additional support fees? (SIS, LMS, rostering)
- What do you mean when you say integrated and can you explain it from a value proposition?
- Can you describe the flow of information between integrated systems?
    - How does the product ensure controlled, secure data sharing?
    - ★ *How is data input validated within AI-enabled tools?*
    - Think about how you should be talking to your customers about this.
- What mechanisms are in place to allow district control of data fields shared and data minimization.
    - ★ *How is direct control and minimization specifically addressed within AI-driven systems?*
- How does the system minimize the need for manual data entry and prevent data duplication?
- *How would you describe the practices used to ensure data privacy, security and integrity within integrated AI system data flows?*

Training

- What is the overall philosophy and approach to client success support in regards to training during onboarding and implementation? How is this support adapted as the district continues to use or expand the use of the product?

- *For products that utilize AI, how do you ensure all your customer facing representatives can articulate how data is utilized and the limitations around AI-driven decision making?*

    - *How are the data utilization and limitations communicated to schools?*

- How are onboarding and professional development resources made available for educators, students, and support staff? What is your process to ensure that these resources meet the need of the targeted roles (e.g., teachers, administrators, IT staff, students)?

- How do you assist districts in the analysis of usage and progress data needed to inform further training needs or identify usage gaps? If needed, are districts able to customize your training?

- *What is your role in ensuring school staff have the AI literacy skills necessary to effectively and responsibly utilize your products?*

Privacy

- If the product is available to the general public, how are the terms of service and privacy policy differentiated for educational institutions? What is your approach to ensuring your terms and privacy policy are education friendly and ensure that districts maintain direct control of student data?

- How would you articulate the privacy controls from a product design perspective? How is this maintained throughout the product lifecycle? How is it articulated within the company? Are districts involved in the development or review of these controls?

- *Do you use an AI Nutrition Label? If not, how do you communicate how AI utilizes data and methods of data minimization, de-identification and pre-sanitization?*

- What controls or processes are in place to ensure that districts can fulfil their obligations under FERPA for student records access, data correction and data deletion? How are districts involved in the development of these controls and processes?
    - *How do you ensure that identifiable data is not unintentionally disclosed in generative AI responses?*
    - *How do identify and facilitate access to student records within generative AI products?*

- What measures are in place to ensure that new technical developments are in line with the agreed upon contract and privacy standards prior to implementation? Are districts engaged in discussions prior to the release of new features that utilize data in a different way?

Accessibility

- How does the product(s) ensure alignment with WCAG 2.1 AA and Section 508 standards? What accessibility features are/are not available?

    - *How are students with disabilities and diverse backgrounds represented within the training data of all AI systems?*

- What processes are in place to ensure that the product is periodically reviewed and tested for accessibility compliance? Are students and/or individuals with disabilities involved in the development and review processes?

- *How do you ensure that AI-generated content and recommendations appropriately address student needs and any biases are clearly identified and communicated to schools?*

- *How might you articulate how AI tools adapt content and interfaces for user disabilities/abilities and what customizations are available for individual learners?*

- If a school has a concern about accessibility within the product or its integrations with other systems, what is the process to report and address these concerns?

Safety

- What is your approach to and established safeguards for ensuring that age-appropriate content is consistently delivered?

  - Can you articulate how advertisements are managed or if they are eliminated in student-facing environments?

  - *How would you articulate the approach to student safety when using LLMs for AI-enabled features? Specifically, how might you address concerns regarding potential bias or inappropriate content/suggestions in generated responses?*

- How does the product(s) support safe use across all student age groups including? How are schools involved in the oversight and customization of safety settings and communication tools?

- How do you ensure that safety policies and response protocols for unsafe interactions and content are easy to navigate and available for schools?

- *If a monitoring or analytic tool utilizes generative AI, what special considerations are given to ensure accuracy and effectiveness of responses that may impact student safety?*

Security

- What established cybersecurity standards (e.g., NIST, CIS) is the product aligned with and what safeguards are in place to protect against unauthorized access, data breaches, and cyber threats?

- How would you address school concerns regarding cybersecurity and the potential of a data breach? Can you speak to data security measures including encryption, transmission protocols, secure authentication and security audits?

- *AI systems have unique security vulnerabilities, how might you address a school's concerns regarding these risks? Who within your organization can answer questions about the potential of data poisoning, adversarial attacks and cybersecurity risk mitigation?*

- How is data access limited based on user roles and responsibilities within the school and with service provider staff?

- What should districts expect in the event of a security incident or data breach? What are the roles within the service provider, what are the expectations of the school?

Effectiveness

- How is the effectiveness of the product measured and how might you communicate the value of investment to a school?
- What research and evidence is available to demonstrate effectiveness of the program for a diverse range of learners including those with disabilities, learners at all academic levels, and varied backgrounds?
    - *Are there any data sets that speak to the effectiveness of the AI tools integrated into the system separate from the overall product effectiveness? Do these data sets assess effectiveness for a variety of learner backgrounds, abilities and academic levels?*
- How might you communicate the product's ability to meet a variety of learning styles and instructional approaches in educational terms?
- How can a school use the tools available to monitor the fidelity of implementation and student progress towards established learning objectives?
- What tools and processes are used internally to ensure the product continues to remain effective for all learners? If effectiveness varies for specific subgroups, how are these variances articulated to the school?
- *How do you approach conversations around the inherent risks and biases that exist within AI tools? What measures are incorporated to help mitigate these risks?*

Sustainability/Scalability

- What is your approach to customer success? How is this accomplished through technical support, documentation, and training?
- How do you ensure current and future product features are compatible with common devices used in schools? How might you handle a request from a school that uses a device that is not fully supported? *Does this process differ when AI tools are involved?*
- What process do you have in place to ensure that the product/implementation scales effectively from pilot to full implementation? Consider what differentiates a pilot from implementation. Is there a difference in contracting, data handling, support or available features?
- How does the product roadmap demonstrate long-term viability and how are updates and patches released and communicated to schools? *How might this process differ with changes in data utilization and the integration of AI tools or other emerging technologies?*

- What strategies exist within product development to ensure the product remains relevant, effective and addresses all components of the IT PASSES framework?

** Indicates an AI focused discussion*