

WS-DPS: DATA PRIVACY / SECURITY / GOVERNANCE

Draft Deliverables for Meeting 4 Convergence Gate

Prepared by Jillian Burkley for John Black

FCCPS AI in Schools Ad Hoc Advisory Committee

February 2026 — DRAFT v0.1 for Co-Lead Review

Purpose of This Document

This package includes draft versions of all three WS-DPS deliverables required for the March 6 convergence gate, along with the readiness checklist. It draws on frameworks from my doctoral capstone (AIEIP), adapted for the FCCPS context. Everything here is a starting point for our co-lead discussion — I want your input on structure, scope, and FCCPS-specific adjustments before we finalize.

Deliverable 1: AI Tool / Data Risk Categories

Requirement: "Tool/data risk categories (plain language) + minimum requirements by category"

Risk Tier Framework

Every AI tool used in FCCPS classrooms or operations would be classified into one of three tiers based on how it handles student data. Each tier triggers a different level of review and approval.

TIER 1 — LOW RISK: No Student Data

What this means: The tool does not collect, store, or process any student-identifiable information. Students may or may not interact with it directly, but no personal data flows to the vendor.

Examples: AI-powered lesson plan generators used only by teachers; AI image generators for creating classroom materials; grammar/style checkers used on teacher-authored content.

Minimum Requirements:

- Teacher verifies no student data is entered into the tool
- Tool is documented in department/school AI tool inventory
- Basic review by department lead or instructional coach

Approval: Department/building-level approval. No DPA required.

TIER 2 — MODERATE RISK: Anonymized or Aggregated Data

What this means: The tool processes student work or interaction data, but in anonymized or aggregated form. No individual student can be identified from the data the vendor receives.

Examples: Classroom response/polling tools with anonymous mode; AI-assisted formative assessment tools using de-identified data; writing feedback tools where student names are stripped.

Minimum Requirements:

- Vendor confirms anonymization/aggregation methodology in writing
- Data Processing Agreement (DPA) reviewed and signed
- Data retention policy documented (vendor must specify how long data is held)
- Annual review of vendor compliance
- FERPA compliance verification

Approval: District-level review (IT + curriculum). DPA required.

TIER 3 — HIGH RISK: Identifiable Student Data

What this means: The tool collects, stores, or processes personally identifiable student information (PII). This includes any tool where a student logs in with a school account, where the vendor can link data to a specific student, or where sensitive records are involved.

Examples: Adaptive learning platforms (e.g., IXL, Khan Academy); AI tutoring systems with student accounts; any tool integrated with the SIS or LMS; AI tools used in IEP/504 planning or progress monitoring.

Minimum Requirements:

- Signed DPA with explicit data handling, retention, and deletion terms
- FERPA, COPPA (if applicable), and Virginia student data privacy law compliance verified
- For tools touching IEP/504 data: IDEA compliance review + explicit parental/guardian consent
- Vendor security assessment (encryption, access controls, breach notification procedures)
- Algorithmic bias assessment for any tool making recommendations about students
- Human-in-the-loop requirement for any consequential decisions (placement, grading, intervention)
- Data deletion confirmation process when tool is discontinued
- Semi-annual compliance audit

Approval: District-level review (IT + curriculum + administration + legal). Full DPA + security review required. Pilot period recommended before broad deployment.

Special Consideration: Students with Disabilities

AI tools used with students receiving SPED services require heightened scrutiny regardless of tier. The following data categories are especially sensitive and trigger additional requirements:

- **IEP/504 plan data:** Disability classifications, accommodations, modifications, and progress monitoring data. IDEA requires these records receive protections beyond standard FERPA requirements.
- **Adaptive technology usage patterns:** Data from assistive tech tools may reveal disability-related information even when not explicitly labeled as such.
- **Behavioral data from AI tools:** AI-driven behavior monitoring systems may flag behavioral differences in culturally diverse students or students with emotional/behavioral disabilities as problematic (Maslej et al., 2023), creating risk of bias-driven consequences.
- **Accommodation records:** AI systems that process accommodation data could inadvertently create profiles that follow students beyond intended educational contexts.

Additional requirement: Any Tier 2 or Tier 3 tool used with SPED populations must include an accessibility review (assistive tech compatibility, UDL alignment) and an algorithmic bias assessment focused on disability-related outcomes.

Deliverable 2: Procurement / Governance Decision Checklist

Requirement: "A short procurement/governance decision checklist (what must be true before adoption)"

This checklist is designed for any FCCPS staff member, administrator, or department considering adopting a new AI tool. It answers one question: Can we use this tool? Every item must be confirmed before the tool can move forward at its designated tier.

Step 1: Classify the Tool

Question	If YES →
Does the tool collect, store, or process any student-identifiable information (names, IDs, login data, work samples linked to students)?	Tier 3 — proceed to full review
Does the tool process student work or interaction data in anonymized or aggregated form?	Tier 2 — proceed to standard review
Does the tool have no contact with student data at all?	Tier 1 — proceed to basic review
Will the tool be used with students receiving SPED services (IEP/504)?	Add SPED review layer (any tier)

Step 2: Verify Before Adoption

All items must be confirmed for the relevant tier. Items marked with ★ are non-negotiable across all tiers.

What Must Be True Before Adoption	Tier 1	Tier 2	Tier 3
★ Tool is documented in FCCPS AI tool inventory	✓	✓	✓
★ Staff member can articulate educational purpose and how the tool supports student learning	✓	✓	✓
★ No student data is entered into the tool without appropriate authorization	✓	✓	✓
Vendor confirms anonymization methodology in writing	--	✓	✓
Data Processing Agreement (DPA) reviewed and signed	--	✓	✓
Data retention and deletion policy documented	--	✓	✓
FERPA compliance verified	--	✓	✓

Vendor security assessment completed (encryption, access controls, breach notification)	--	--	✓
Algorithmic bias assessment completed for any tool making recommendations about students	--	--	✓
Human-in-the-loop confirmed for consequential decisions (placement, grading, intervention)	--	--	✓
COPPA compliance verified (if tool is used by students under 13)	--	--	✓
Pilot period completed with documented outcomes before broad deployment	--	--	✓
SPED ADD-ON: IDEA compliance review + parental consent for IEP/504 data	If SPED	If SPED	If SPED
SPED ADD-ON: Accessibility review (assistive tech compatibility + UDL alignment)	If SPED	If SPED	If SPED

Deliverable 3: Top Risks, Mitigations & Suggested Owners

Requirement: "Top risks + mitigations + suggested owners"

RISK 1 Severity: HIGH	Unvetted AI Tools Processing Student Data Without Governance Without a structured approval process, teachers and staff may adopt AI tools that collect student PII without signed DPAs, creating FERPA violations and data exposure risk. Research shows no standardized regulations currently address AI-specific risks in K-12 education (DOE, 2023; Roschelle et al., 2024).
Mitigation	Implement the tiered approval process (Deliverable 1). Maintain a district-wide AI tool inventory. Require DPA review for all Tier 2/3 tools. Communicate clear policy that unauthorized tool adoption is prohibited.
Owner	IT Department (tool inventory + DPA management) + Building Administrators (enforcement)

RISK 2 Severity: HIGH	IEP/504 Data Exposure Through AI Tools SPED students' sensitive diagnostic information, behavioral data, and learning accommodations are increasingly processed through AI systems that may lack adequate safeguards (Roschelle et al., 2024). IDEA requires protections beyond standard FERPA, and AI tools were not designed with these requirements in mind (Haque & Li, 2024).
--	--

Mitigation	SPED add-on review layer for any tool used with IEP/504 students. Explicit parental/guardian consent for AI processing of disability-related data. Prohibit sharing IEP/504 data with AI vendors without IDEA compliance review. Regular audits of AI tools used in SPED contexts.
Owner	SPED Director + IT Department (joint oversight) + Legal Counsel (IDEA compliance review)

RISK 3 Severity: MEDIUM	Algorithmic Bias in Student Assessment and Intervention AI systems misclassify students with disabilities from marginalized backgrounds at rates up to 32% higher than peers (Nguyen et al., 2023). AI-driven behavior monitoring may flag cultural behavioral differences as problematic (Maslej et al., 2023). This can reinforce historical overrepresentation of students of color in certain disability categories.
Mitigation	Require algorithmic bias assessment for all Tier 3 tools. Establish routine bias audits with specific focus on outcomes for students with intersecting marginalized identities. Human-in-the-loop requirement for all consequential decisions. Review disaggregated outcome data annually.
Owner	Curriculum & Instruction (bias audits) + SPED Director (disability-specific review) + Equity Office (intersectionality lens)

RISK 4 Severity: MEDIUM	Tool Proliferation Without Central Oversight Without a centralized inventory and approval process, individual teachers and departments may independently adopt AI tools, creating an unmanageable landscape of vendor relationships, inconsistent data practices, and compliance gaps that IT and administration cannot effectively monitor.
Mitigation	Maintain centralized AI tool inventory. Require all AI tool adoptions to go through tiered approval. Conduct annual audit of tools in use across the district. Establish clear communication channels for staff to request new tools.
Owner	IT Department (inventory + technical review) + Curriculum & Instruction (educational value assessment)

RISK 5 Severity: MEDIUM	Vendor Data Practices Beyond District Control AI vendors may change their data practices, terms of service, or AI model training approaches after adoption. Student data used to train commercial AI models without consent represents a significant and evolving privacy concern.
Mitigation	DPAs must include clauses prohibiting use of student data for model training. Require vendor notification of material changes to data practices. Establish annual vendor compliance review. Include data deletion requirements when contracts end.
Owner	IT Department + Legal Counsel (DPA management and enforcement)

Meeting 4 Readiness Checklist

From John's orientation email, each workstream needs these items ready for the convergence gate:

3 Non-Negotiable Constraints / Guardrails

1	No AI tool may process identifiable student data without a signed Data Processing Agreement and completion of the tiered review process.
2	IEP/504 data must never be shared with AI vendors without explicit IDEA compliance review and parental/guardian consent. This is a federal requirement, not a policy choice.
3	All AI tools used for consequential decisions about students (placement, grading, intervention, behavioral assessment) must include human-in-the-loop oversight. AI recommendations inform — they do not decide.

3 Decision Points / Tradeoffs for Committee Resolution

#	Tradeoff	Options for Committee Discussion
1	Approval Speed vs. Thoroughness How strict should the tool approval process be? Faster adoption means teachers get tools sooner; thorough vetting means fewer risks but potential delays.	<ul style="list-style-type: none"> Option A: Streamlined process for Tier 1/2, full review only for Tier 3 Option B: Full review for all tiers (slower but more consistent) Option C: Pre-approved tool list with expedited review for tools on the list
2	Approved List vs. Criteria-Based Evaluation Should FCCPS maintain a curated list of pre-approved AI tools, or use criteria-based evaluation to assess any tool on demand?	<ul style="list-style-type: none"> Option A: Maintained approved list (clear, but requires ongoing curation) Option B: Criteria-based (flexible, but more work per request)

		<ul style="list-style-type: none"> Option C: Hybrid — approved list for common tools + criteria pathway for new requests
3	Compliance Monitoring Ownership Who owns ongoing compliance monitoring after a tool is approved? This has significant resource implications.	<ul style="list-style-type: none"> Option A: IT Department (technical focus) Option B: Curriculum & Instruction (educational focus) Option C: Shared responsibility with clear RACI matrix

Dependencies from Other Workstreams & FCCPS Staff

What We Need	From Whom	Status
Existing DPA templates and procurement workflows	FCCPS IT / Jerrod Anderson or Bethany Henderson	Not yet requested
Current AI tool inventory (what's already in use)	FCCPS IT Department	Not yet requested
IT capacity for ongoing compliance monitoring	FCCPS IT Department	Not yet requested
Draft policy principles (from Meeting 3)	Full committee (Feb 20 output)	Pending Meeting 3
Policy language alignment	Policy/Recommendation Drafting workstream (David Berol)	Not yet started
Virginia student data privacy law specifics	FCCPS Legal Counsel	Research in progress

Discussion Questions for Co-Lead Check-In

These are the key questions I'd like to work through in our first sync:

On Structure & Scope

1. Does the 3-tier model feel right for FCCPS, or should we adjust the categories? Are there tool types that don't fit cleanly?
2. Is the SPED add-on layer the right approach, or should SPED considerations be embedded directly into the tiers rather than as an overlay?
3. The governance checklist is designed for staff and administrators. Is that the right audience, or do we also need a version for the procurement/IT team?

On FCCPS-Specific Context

1. Do you have contacts for FCCPS IT or procurement who can share existing DPA templates and the current tool landscape?
2. Are there AI tools FCCPS is already using or evaluating that we should use as test cases for the checklist?
3. What's your sense of the committee's appetite for the tradeoffs in the decision points? Are there other tradeoffs you think we're missing?

On Division of Labor

1. **My proposal:** I continue drafting the checklist and risk tiers (building from my AIEIP work), and you review for technical accuracy and FCCPS-specific adjustments. Does that division work for you?
2. Can we establish a weekly async rhythm?
1. **My proposal:** I plan to continue drafting the checklist and risk tiers (building from my AIEIP work) and would like you to review for technical accuracy and FCCPS-specific adjustments. Are there certain days that work best for you to review or collaborate? Please let me know your preferred days.
3. Are there specific sections you'd like to own or contribute to directly?

Source: AIEIP Framework

The frameworks in this document draw from my doctoral capstone, the Artificial Intelligence Ethical Integration Program (AIEIP), developed at Simmons University. AIEIP establishes a comprehensive ethical and compliant framework for AI in special education settings, grounded in:

- **DEIPAR Framework** (Diversity, Equity, Intersectionality, Power, and Anti-Racism) — ensures that social justice remains central to AI governance. I understand we may not be able to display this with our current administration, and it can be adaptable with the FCCPS vision and mission.
- **Diffusion of Innovations Theory** — guiding phased implementation and adoption strategies
- **FERPA, IDEA, and Section 504 compliance protocols** — translated into actionable guidelines for educators
- **AI Bias Audit methodology** — routine assessment processes for identifying disparities in AI-driven decisions