Security & Facilities Brief

For District IT Directors, Data Privacy Officers, and Facilities Management

This brief addresses the technical, security, and facilities concerns regarding MuggsOfLearning's teacher-managed AI subnet. The system is designed as a collaborative pilot with full deference to district leadership on all decisions.

1. The Secure Edge Gateway

The classroom connects to the school's network through a dedicated Secure Edge Gateway — not a personal router plugged into a wall jack. Student traffic is physically and logically separated from the district's backbone.

- **WAN In:** Ethernet from the school's network drop.
- **NextDNS:** Intercepts all DNS queries at the gateway, enforcing CIPA-compliant filtering before data reaches student workstations.
- **LAN Out:** Filtered connection via ICS to local router.
- **Router (AP Mode):** Distributes filtered connection to offline-capable student Mini PCs.

This is deploying a Secure Edge Gateway that reduces the district's troubleshooting burden by handling DNS and routing locally. Students confirm the restrictions work.

2. Student Data Privacy (PII)

- **Local-Only Inference:** If the school obtains student workstations, students run Qwen 3.5 9B Q4 locally. Students do receive generative responses, but all inference happens on-device. No data leaves the room.
- **Student Logging:** Students are expected to log AI interactions. Teacher monitors interaction logs for dishonest or irresponsible use.
- **Local Data Residency:** All student work and evaluations stored locally. No data trains third-party models.
- **R.S. 17:3914:** No external data transfers — natively compliant with Louisiana student privacy law. No third-party Data Sharing Agreement required.
- **Zero-Transfer Verification:** NextDNS logs catch unauthorized traffic before it hits the school's switch.

3. Human-in-the-Loop Governance

- **Teacher-as-Gateway:** No AI assessment feedback reaches a student automatically. The Teacher Override Loop requires review and confirmation.
- **Auditability:** Every AI-proposed evaluation is logged alongside the teacher's confirmed version. Transparent audit trail for parent conferences or admin review.
- **AI-Free Composition:** MuggsOfWriting provides a digital "blue book" where generative AI is disabled, ensuring authentic student authorship when required.

4. Gateway Components

Component	Security Benefit
Dual-NIC Mini PC	Physically separates classroom from district WAN
NextDNS CLI	Hardware-level blocking of malware and trackers
Router (AP Mode)	Local connectivity without taxing school Wi-Fi
Cloudflare Tunnel	Optional: Zero Trust outbound-only admin access

5. Strategic Comparison

Corporate edTech	MuggsOfLearning
Requires DSAs + cloud storage	Zero-Transfer. Data stays in room.
Truncates sources for token cost	Full-context. Every source loaded.
Generic engagement metrics	GAT-aligned. Grow/Achieve/Thrive.
SSO integration + whitelisting	Subnet-isolated. Managed gateway.
Adds to district support surface	Self-sustaining. Teacher-maintained.
Per-student licensing fees	Capital hardware. ~400 students.

IT Governance Commitment
All hardware and network configurations subject to review and approval of the District IT Director.

Hardware Specifications

Teacher Tier: Two Custom-Built GPU Rigs

Each rig is a custom build with its own power supply, cooling, and UPS. Neither has manufacturer BIOS serial numbers burned onto the motherboard (see Network note).

RIG 1	**RTX 4090**	Custom build · ~650W peak · 96GB DDR5 · Intel Core Ultra 9
RIG 2	**RTX 5070 Ti**	Custom build · ~450W peak · Dedicated inference rig

Power & Electrical

- **Combined Peak:** ~1,100W across both rigs. Within capacity of two standard 15-Amp/120V circuits.
- **UPS:** Each rig on a dedicated UPS with surge protection.
- **Student PCs:** ~65W each. 30 units on one shared circuit.

Thermal & Acoustic

- **Cooling:** Air or AIO liquid cooling per rig. Stable temps.
- **Noise:** Inference bursts comparable to a classroom projector.
- **Placement:** 6 inches wall clearance per rig. No enclosed cabinets.

Network Connectivity

Custom builds lack manufacturer BIOS serial numbers on the motherboard. This prevents authentication on Wi-Fi networks using MAC/BIOS device registration. Student Mini PCs are consumer-grade (not enterprise/ed editions), presenting similar registration challenges.

- **Current Solution:** Dual-NIC gateway with NextDNS. More restrictive than school Wi-Fi. Students confirm.
- **Without Tunnel:** 3 Ethernet ports required if no dedicated subnet (1 gateway + 1 per GPU rig).
- **With Subnet:** All devices connect directly to the school network with NextDNS filtering at the gateway.
- **Deference:** The teacher adapts to whatever the District IT Director approves.

Student Workstations

Solid-state Mini PCs designed for efficiency and durability.

- **Power:** Less than 65W each. 30 on one circuit.
- **Inference:** Qwen 3.5 9B Q4 runs locally. No high-speed internet bandwidth required.
- **Security:** BIOS-level protections against unauthorized software installation.

Component Summary

Component	Function	Facilities / IT Impact
GPU Rig 1 (RTX 4090)	Primary AI inference	1 outlet + Ethernet; standard ventilation; ~650W peak
GPU Rig 2 (RTX 5070 Ti)	Secondary AI inference	1 outlet + Ethernet; standard ventilation; ~450W peak
Dual-NIC Gateway	Secure Edge Gateway / ICS	Low power; separates classroom from district WAN
Router (AP Mode)	Local distribution	Low power; distributes filtered connection
Mini PCs (×20–30)	Student workstations	~65W each; no network strain; local inference
UPS Units (×2)	Power conditioning	Surge protection for each GPU rig
NextDNS	Content filtering	Hardware-level CIPA compliance; more restrictive than student Wi-Fi

What the School Provides

The school provides:

- A dedicated classroom (not shared/rotating)
- Standard electrical (two 15-Amp circuits preferred)
- One Ethernet drop (three if no dedicated subnet)
- Student workstations (teacher specs and configures)
- A teaching position + planning time

Sean provides:

- Teacher-tier GPU rigs (RTX 4090 + 5070 Ti)
- Networking equipment (gateway, router, UPS)
- All software, AI models, prompt architecture
- Workstation configuration and maintenance
- No licensing fees. No vendor contracts.

IT Governance Commitment

All hardware deployments, network configurations, and security policies are subject to the review and approval of the District IT Director.