CASE STUDY

A school locked out of its own website. Now it owns it.

Academy of Academic Excellence, a private elementary school in Richmond, Virginia.

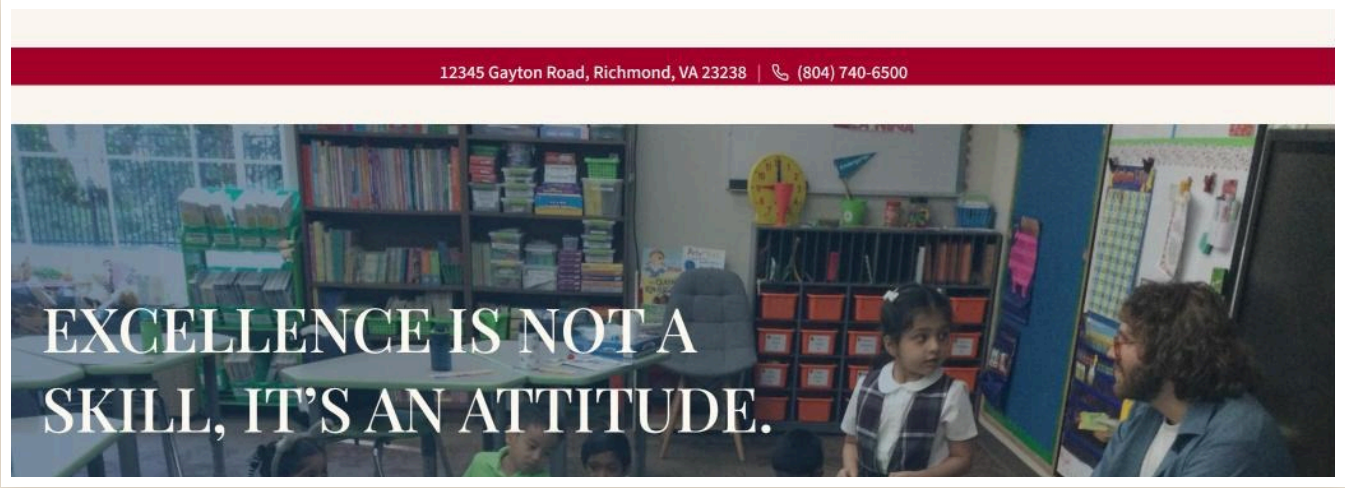
The problem

- The site sat on the same host for about 30 years with no upkeep.
- The old web vendor was sold off, and the site was damaged.
- The school lost access to its own WordPress account.
- The online application and intake forms were gone.

Families were landing on a site that didn't work. Nobody on staff could get in to fix it.

What I did

1. Got the site and content back.
2. Gave the school back its own logins.
3. Moved hosting, with a plan for the site and email.
4. Built a new homepage and rewrote content.
5. Set up forms that send to the school's inbox.
6. Handed over every login, written steps, and shared folders.



The new homepage at academy-of-excellence.com: clear message, address and phone up top, two next steps for parents.

What changed

BEFORE	AFTER
Locked out of their own site	Full access, every login in the school's hands
One person held all the passwords	Logins documented and owned by the school
Application forms gone	Forms that land in the school's inbox
No one knew how it worked	Written steps and shared folders for staff

WHY THIS MATTERS NOW

Protecting kids now includes protecting their data.

The website job taught me something bigger. When one person holds the keys and nobody has a plan, a school is one bad day from losing control. Here in Richmond, we just watched that happen at scale.

Richmond Public Schools went offline after a cyberattack.

It started Oct. 21, 2026. The district took the internet offline across all schools, and the FBI is now working with RPS. As of Oct. 31, officials were still checking whether personal information was affected.

Sources: WTVR, Oct. 31, 2026; WWBT 12 On Your Side, Oct. 22 and Oct. 29, 2026

This is common, not rare.

A Center for Internet Security study of more than 4,600 schools and districts found 82% of K-12 organizations experienced cyber threat impacts over 18 months.

Source: Center for Internet Security, 2025

Virginia now has a law on AI in schools.

Virginia Code § 22.1-20.2:1 (2026) directs the Department of Education to post guidance on safe AI use in classrooms, covering student data privacy (FERPA and COPPA), teacher training, and data agreements that stop student data from training outside AI models. Every public school board must set policies that match it.

Source: Code of Virginia § 22.1-20.2:1; VPM, Mar. 25, 2026

Private schools aren't bound by that law. But parents will expect the same protections, and most small schools don't have a tech person to make it happen.

AI training that goes beyond prompting

Most AI training shows staff how to type a question. That's the easy part. I teach your team how to use AI safely, by role:

Administrators

An AI use policy in plain words. Which tools are allowed, who approves new ones, and what to do when something goes wrong.

Teachers

Using AI for lesson prep, feedback, and parent emails without putting student names, grades, or IEP details into it.

Front office

Spotting phishing emails, managing passwords and logins, and handling parent data the right way.

The whole school

A list of every tool that touches student data, who owns each login, and a simple plan for a bad day.

WORK WITH ME

Clear scope. Clear prices.

Every engagement starts with a free 30-minute call to confirm fit and scope it honestly, before any money changes hands.

OFFER	WHAT YOU GET	INVESTMENT
Staff Training Day	A half-day, hands-on AI literacy and safety workshop using the tools your school already has	**~$2,500**
Infrastructure & Training Package	A full audit of your site, hosting, forms, and scheduling tools, one staff training session, and a written findings report	**$3,500–$6,000**
Full District Rollout	Implementation across departments, scoped by consultation	**Up to ~$27,000**

Add-ons, priced separately

ADD-ON	INVESTMENT
Admissions and intake workflow, built and working	**$1,500–$2,500**
Google Drive, forms, and scheduling set up so staff can find things	**$750–$1,500**
Homepage or content rebuild	**Quoted after the call**

Who I am

I'm Tonia Emanuel, founder of Coach You 360 in Richmond. I spent 15 years at Allscripts/Veradigm in healthcare technology, including about 10 years as a Senior Client Success Manager. I'm not a cybersecurity firm. I fix the basics, train your people, and tell you when you need one.

Start with a 30-minute call.

I'll look at what you have and tell you what's working, what isn't, and what to fix first.

BOOK YOUR CALL →

coachyou360.com/schools · tonia@coachyou360.com · 804-508-4755

Truth → Shift → Move Different

Sources

WTVR, "Richmond schools work with FBI, state police to restore systems after cyberattack," Oct. 31, 2026
WWBT, "Richmond Public Schools turns to FBI, third party after cyberattack," Oct. 29, 2026
WWBT, "Richmond schools remain offline as cybersecurity incident investigation continues," Oct. 22, 2026
Center for Internet Security, "CIS Study Finds 82% of K-12 Organizations Experienced Cyber Threat Impacts in the Past 18 Months," 2025
Code of Virginia § 22.1-20.2:1 (2026, cc. 937, 943)
VPM, "Spanberger to consider legislation requiring state guidance on AI in schools," Mar. 25, 2026