

IKON INSIGHTS

TECHNOLOGY NEWS FOR K-12 SCHOOLS

Brought to you by IKON EduTech Group, Inc.



IN THIS ISSUE

- Blended Funding: How schools Can Accelerate Tech Upgrades
- The Growing Quishing Security Threat: Is Your School at Risk of a QR-Code Compromise?
- School Tech Success Starts Here: 7 Traits of a Top-Notch IT Company
- Webinar: What if E-Rate Goes Away? How to Stack Technology Grants

This monthly publication provided courtesy of IKON EduTech Group.

IKON is a premium IT consulting company focused on providing K-12 schools with customized technology solutions and personalized support.

Get More Free Tips, Tools and Services on Our Website:

www.ikonbusinessgroup.com
(212)334.6481

BLENDED FUNDING: HOW SCHOOLS CAN ACCELERATE TECH UPGRADES

When the federal budget lens is blurry, many tech directors hit pause. But classrooms can't wait for Wi-Fi, cybersecurity, or emergency-alert systems to maybe appear in next year's appropriations bill. The good news? You don't have to sit on the sidelines. By blending several smaller, better-defined funding streams—think E-Rate, ESSA, state safety grants, even vendor incentives—you can keep network refreshes and student-safety projects on track today instead of next September. Blended funding isn't about chasing the biggest pot of money. It's about layering several pots that each solve a specific piece of the puzzle.

WHY THE CLOCK MATTERS

Federal deadlines are marching on, whether we're ready or not:

- **ARP ESSER dollars** must be **obligated by September 30 — yes, of this year** —and fully liquidated 18 months later. Miss the window and the money evaporates.
- **E-Rate Funding Year 2025** closed its Form 471 window in March. Funding Commitment Decision Letters will start landing this summer, but you can already be sketching your next application for FY 2026.
- State safety and STEM grants reset every spring, and many announce winners on a rolling basis throughout June and July.

That cadence creates a powerful rhythm: spring for planning, summer for purchasing, fall for implementation, and winter for auditing impact. Schools that align their board calendars to that rhythm rarely lose a funding opportunity.

(continued on page 2)

BLENDING FUNDING: HOW SCHOOLS CAN ACCELERATE TECH UPGRADES

(continued from page 1)

BLENDING FUNDING, DEMYSTIFIED

Blended funding means braiding two or more restricted streams (federal, state, local, philanthropic, or private) into a single, board-approved project. Instead of chasing one big grant, leaders layer several smaller pots that each pay for an eligible slice.

At its heart, blended funding is simple: match each line on your tech roadmap to at least two funding sources so no single grant controls your timeline. For example:

Funding Source	Typical Use-Case	Pair With
E-Rate Cat 2	Core & edge network, Wi-Fi 6E, filters, firewall subscriptions	ESSA Title IV-A for PD on new tools
ESSA Title IV-A	STEM kits, esports labs, digital citizenship programs	Local capital bonds for facility upgrades
State Safety Grants	Panic-alarm systems (Alyssa's Law compliance), cameras	E-Rate Cat 1 broadband for backhaul
Philanthropic & Vendor Gifts	Devices, charging cabinets, ergonomic gear (e.g., IKON + Kensington program)	Local PTO funds for accessories

MAP YOUR 12-MONTH FUNDING CALENDAR

Imagine it's April. Your leadership team finalizes the tech plan and flags three high-priority needs: network hardening, classroom displays, and an Alyssa's Law-compliant alert system.

Quarter	Critical Period	What to Do
Q2 (Apr-Jun)	State budgets finalize; Title IV-A allocations posted	Build purchase orders that match each grant's stated purpose & budget line.
Q3 (Jul-Sep)	ESSER obligation deadline; Back-to-school vendor promos	Lock in hardware quotes before September price hikes; submit board resolutions.
Q4 (Oct-Dec)	Prep season for E-Rate FY 2026	File Form 470 by Thanksgiving; conduct bid evaluations and board approvals.
Q1 (Jan-Mar)	E-Rate Form 471 window & many state safety-grant deadlines	Bundle network & security SKUs under one 471; submit supplemental grant apps.

Following this drumbeat means you never find yourself staring at idle Chromebooks because the firewall refresh missed a grant deadline.

QUICK-WIN PROJECTS THAT QUALIFY RIGHT NOW

- **Network Hardening + Cyber Insurance Readiness**
 - Fund 85 % of switching & firewall refresh with E-Rate.
 - Use leftover ESSER cash for multi-factor authentication rollout.
- **Device & Display Refresh**
 - Leverage vendor buy-back credits plus Title IV-A for STEM cart pilot.
- **Emergency Communications (Alyssa's Law)**
 - Pair state safety dollars with E-Rate Cat 1 for redundant LTE circuits.
- **Cybersecurity Managed Services**
 - Combine local operating budget (recurring) with NY CIPS grant (first-year lift).



HOW IKON EDUTECH GROUP MAKES IT EASY

Navigating grant language, procurement rules, and vendor contracts can feel like a part-time job. IKON's specialists handle E-Rate filings, Grant writing, Preferred-partner pricing and more. In short, we keep the paperwork off your desk so you can keep your eyes on student outcomes.

THE GROWING QUISHING SECURITY THREAT: IS YOUR SCHOOL AT RISK OF A QR-CODE COMPROMISE?

A NEW TWIST ON AN OLD FOE

Cybercriminals have discovered a fresh social-engineering playground in the humble QR code. “Quishing”—phishing that hides malicious links inside QR images—is surging across the education sector. Microsoft now blocks more than 15,000 QR-code-bearing emails aimed at schools every single day. [Microsoft](#)

WHAT EXACTLY IS “QUISHING”?

Quishing repackages classic phishing. Instead of a suspicious blue hyperlink, staff receive a PDF, flyer, or email containing a QR code that supposedly leads to payroll, parcel tracking, or a “required update.” Scanning the image on a phone bypasses most URL filters and lands the victim on a credential-harvesting page before anyone realizes something is wrong. [EdTech Magazine](#)



WHY SCHOOLS ARE PRIME TARGETS

School Reality	How Attackers Exploit It
QR codes are everywhere — from classroom posters to lunch-menu emails.	A forged code pasted over the original or embedded in email looks routine.
Large, diverse user base (students, parents, volunteers).	More potential scanners = larger attack surface.
Budget and staffing constraints in IT security.	Slower patching, limited email-image inspection, and training gaps.

Attackers know QR codes feel helpful and urgent (e.g., “Scan to view time-sensitive payroll change”). That psychological pressure drives quick compliance.

RED FLAGS TO WATCH FOR

- **Out-of-context QR codes** in messages you weren’t expecting, especially those urging immediate action or account verification.
- Codes accompanied by **generic greetings, spelling errors**, or requests for login credentials.
- Codes that resolve to **shortened or misspelled domains** when previewed.
- **Physical QR stickers** that look layered or misaligned on signage.

SEVEN STEPS TO REDUCE QUISHING RISK

1. **Enable image-based email inspection** in Microsoft Defender for Office 365 or equivalent secure-email gateways to detect embedded QR codes.
2. **Train staff and students to preview links** before browsing (most mobile cameras show the destination URL). Embed quishing drills in existing phishing-simulation programs.
3. **Publish a “QR Code Use Policy.”** Require all campus-posted codes to include a plain-text URL nearby and to be generated only through approved accounts.
4. **Turn on multifactor authentication (MFA)** for every cloud service; credential theft is useless if stolen passwords alone can’t open the door.
5. **Lock down personal devices** that access school email with mobile-device-management (MDM) profiles enforcing screen-lock and OS patching.
6. **Segment guest Wi-Fi** so a compromised phone can’t pivot into student-information systems.
7. **Prepare an incident-response runbook** for social-engineering attacks: isolate the account, revoke sessions, notify affected users, and report to MS-ISAC.

BOTTOM LINE

QR codes are here to stay, but the convenience they bring to classrooms also hands cybercriminals a stealthy delivery channel. Proactive controls, clear policies, and a security partner who understands the nuances of K-12 operations are the difference between a quick scan and a costly breach.

HOW IKON EDUTECH GROUP CAN HELP

IKON’s K-12-focused managed-security services combine 24/7 email and endpoint monitoring, staff awareness coaching, and rapid incident response. Schedule a complimentary 30-minute Cybersecurity Audit to see how your current defenses stack up against the latest threats.

SCHOOL TECH SUCCESS STARTS HERE: 7 TRAITS OF A TOP-NOTCH IT COMPANY

IS YOUR IT PARTNER TRULY BUILT FOR K-12? HERE'S HOW TO TELL

Digital transformation isn't just a buzzword in education—it's the backbone of safe, engaging learning. But without the right IT Services Provider at your side, bold tech plans can stall fast. K-12 districts face challenges—FERPA compliance, student data privacy, tight budgets—that most generic vendors simply don't understand.

The right partner speaks your language. They know that a Chromebook outage during statewide testing isn't just inconvenient—it's catastrophic. They treat student information as sacred, enforcing ironclad governance and round-the-clock protection. They also recognize that every district's calendar (and budget) rises and falls with the school year, so their solutions flex accordingly.

So, how do you spot an IT company that's truly K-12-ready? Look for these seven must-haves:

1. **Classroom-Tested Experience** - Proven success supporting districts of all sizes, from rural schools to large urban systems.
2. **Seamless Workflow Integration** - New tools drop neatly into your SIS, LMS, and help-desk flow—no extra clicks for teachers.
3. **Elastic Power & Pricing** - Scale resources up for testing week, down for summer break—billing follows suit.
4. **24/7 Whole-Stack Support** - From firewall alerts at 2 a.m. to projector glitches at 2 p.m., help is always on.
5. **Lock-Tight Data Governance** - FERPA, Ed Law 2-d, and local regs baked into every policy—no offshore loopholes.
6. **Radical Transparency** - Clear SLAs, real-time dashboards, and honest “what happened” reports if things go sideways.
7. **Actionable Insights, Not Just Alerts** - One pane of glass with plain-English analytics your superintendent can share at Monday's board meeting.



Bottom line: If your current provider can't check every box, your district might be settling for “good enough” when students deserve greatness.

READY FOR AN IT PARTNER THAT UNDERSTANDS CLASSROOMS AS WELL AS CODE?

IKON Edutech Group pairs award-winning cybersecurity with white-glove service tailored to K-12. Book a 15-minute consult today and see how we can keep your district secure, scalable, and future-proof.

UPCOMING WEBINAR:

WHAT IF E-RATE GOES AWAY? HOW TO STACK TECHNOLOGY GRANTS

Federal chatter about revising—or even sunseting—E-Rate has many school tech leaders on edge.

In this webinar, we'll map out a proven playbook for combining multiple grants—so your Wi-Fi upgrades, safety systems, and classroom devices never hinge on a single funding source.

E-Rate, ESSER, Title IV-A, and state safety grants each come with hard-lined deadlines and eligibility quirks. The right mix, however, lets you install mission-critical tech this school year—without blowing your capital budget.

If you've ever shelved a network refresh—or an Alyssa's Law alert system—because the funding “wasn't final yet,” this session is for you.

Signup Now



LIVE WEBINAR: June 5th 2025, 11am EST

Can't make it live? Register anyway and we'll send the recording—plus the checklist and matrix—straight to your inbox.