FOR K-12 SCHOOL ADMINISTRATORS, IT DIRECTORS & DISTRICT LEADERS

# The K-12 School Administrator's Guide.

# To I.T. Support and Services.

The owner's guide to IT support for **public districts, charter schools, and private K-12 campuses** in South Florida. FERPA, CIPA, E-Rate, Chromebook fleets, classroom Wi-Fi, and the 21 questions every administrator should ask before signing.

| 10+ | 97% | 24/7 | 9–5:30 |
|---|---|---|---|
| YEARS | RETENTION | SOC SECURITY | OFFICE HOURS |

(844) 919-8534
rrgnetworks.com

CONTENTS

# What's inside.

FROM THE DESK OF HEBER RODRIGUEZ, PRESIDENT

# Technology should serve teachers — not the other way around.

If you run, administer, or are responsible for a K-12 school or district in South Florida — a public district, a charter school, a private or faith-based campus — and you're trying to figure out what good IT support actually looks like, this guide is for you.

I'm Heber Rodriguez, President of RRG Networks Solutions. We've served South Florida businesses and institutions for over 10 years with a 97% client retention rate. K-12 is one of the most demanding IT environments we work in. **You're managing Chromebook fleets, two competing platforms (Microsoft and Google), student data that has federal privacy protections, a content-filtering mandate tied to your federal funding, and a school calendar that makes every maintenance window a negotiation.**

And you're doing most of it with fewer IT staff than a company one-tenth your size.

The most common question we get from school administrators is "What do you charge?" — and it's the wrong question. The right question is what you'll get for what you spend, and what risk you'll carry if you choose poorly. A FERPA breach, a ransomware shutdown during FSA week, or a Wi-Fi failure on state testing day — these aren't hypothetical. They happened to a district near you.

I wrote this guide to help you understand how IT firms package and price services, what K-12-specific compliance looks like from an IT perspective, and how to pick the right firm based on what they actually deliver — not just the number on the proposal.

**Heber Rodriguez**
PRESIDENT · RRG NETWORKS SOLUTIONS

SOUTH FLORIDA'S K-12 IT SPECIALIST

# The team behind 10+ years & 97% retention.

Fortinet-certified network specialists, a 24/7 Security Operations Center for security monitoring, and compliance practices built around FERPA, CIPA, and E-Rate — for schools that can't afford downtime.

RRG Networks Solutions serves South Florida public districts, charter schools, and private K-12 campuses across Miami-Dade, Broward, Palm Beach, Collier, Lee, and Monroe counties. We've been doing this since 2016.

Our team includes full-time engineers and network specialists, supported by a 24/7 Security Operations Center for real-time threat monitoring. We're known for taking on complex multi-campus, multi-platform environments — from a small charter with 200 students and no IT staff to a district with thousands of devices and an IT director who needs a co-managed partner.

Our cybersecurity practice aligns with FERPA, CIPA, COPPA, PPRA, NIST 800-171, HIPAA, and PCI DSS. We're familiar with Florida FDOE reporting requirements and the CISA K-12 cyber guidance. Our security posture is audited recurringly by Galactic Advisors.

BY THE NUMBERS

## What 10+ years looks like.

| | | |
|---|---|---|
| 10+ | YEARS IN BUSINESS | Serving South Florida since 2016. |
| 97% | CLIENT RETENTION | Year over year. We earn it monthly. |
| 24/7 | SECURITY OPS CENTER | Real-time threat monitoring. |
| 9–5:30 | OFFICE HOURS | Live support Mon–Fri. After-hours emergency coverage available. |

**Compliance: FERPA · CIPA · COPPA · PPRA · NIST 800-171 · HIPAA · PCI DSS · FL K-12 Cyber · E-Rate**

EVERY KIND OF K-12 ENVIRONMENT IN SOUTH FLORIDA

# Built for your type of school.

Public districts, charter schools, and private campuses each have different IT needs, compliance obligations, and budget realities. We've worked in all three.

PUBLIC DISTRICTS

## District-Scale Operations

FERPA · CIPA · E-Rate. Co-managed alongside your IT director — not around them. We take the help desk, after-hours coverage, summer projects, and cybersecurity operations. The director keeps strategic ownership: vendor relationships, board reporting, instructional-tech direction.

**Key concern:** Ransomware readiness, FSA testing window stability, and E-Rate filing coordination.

CHARTER SCHOOLS

## Mission-Driven, No Internal IT

Your full IT team for the cost of one hire. Charter schools often have 200–800 students, an operations director wearing every hat, and an authorizer that expects a clean renewal package. We scope to what your authorizer actually expects and what your ops director can own day-to-day.

**Key concern:** FERPA exposure, Chromebook fleet management, and MFA for every adult account.

PRIVATE & FAITH-BASED

## Smaller Campus, High Expectations

Smaller campuses with premium expectations around student data and parent trust. Private schools don't receive E-Rate funding but still carry COPPA and FERPA-equivalent obligations, and parents expect the same data-protection standards as any public school.

**Key concern:** Student data protection, parent portal security, and classroom device reliability.

BOTTOM LINE

**Whatever your school type, the IT problems are the same. What changes is the budget, the authorizer, and who's on the other end**

SOUND FAMILIAR?

# If any of these sound like your week, you're not alone.

## THE 5 BIGGEST K-12 IT PAIN POINTS

| 01 | 02 | 03 | 04 | 05 |
|---|---|---|---|---|
| Ransomware shut down the district next door | Teachers juggle Microsoft AND Google every period | Wi-Fi specced for 30. State testing brought 800 devices online. | FERPA breach in 6 clicks, on a Tuesday afternoon | One IT director. 800 staff. 3,000 students. |

→ *A third-grade class sat through fifteen minutes of frozen Chromebooks during their first reading assessment. The kids don't get that time back.*

→ *A parent emails the principal: their child's portal is showing another student's data. You have 24 hours to figure out whether it's a FERPA breach.*

→ *Ransomware note on the principal's laptop. Board meeting is Thursday. Local TV is already calling for comment.*

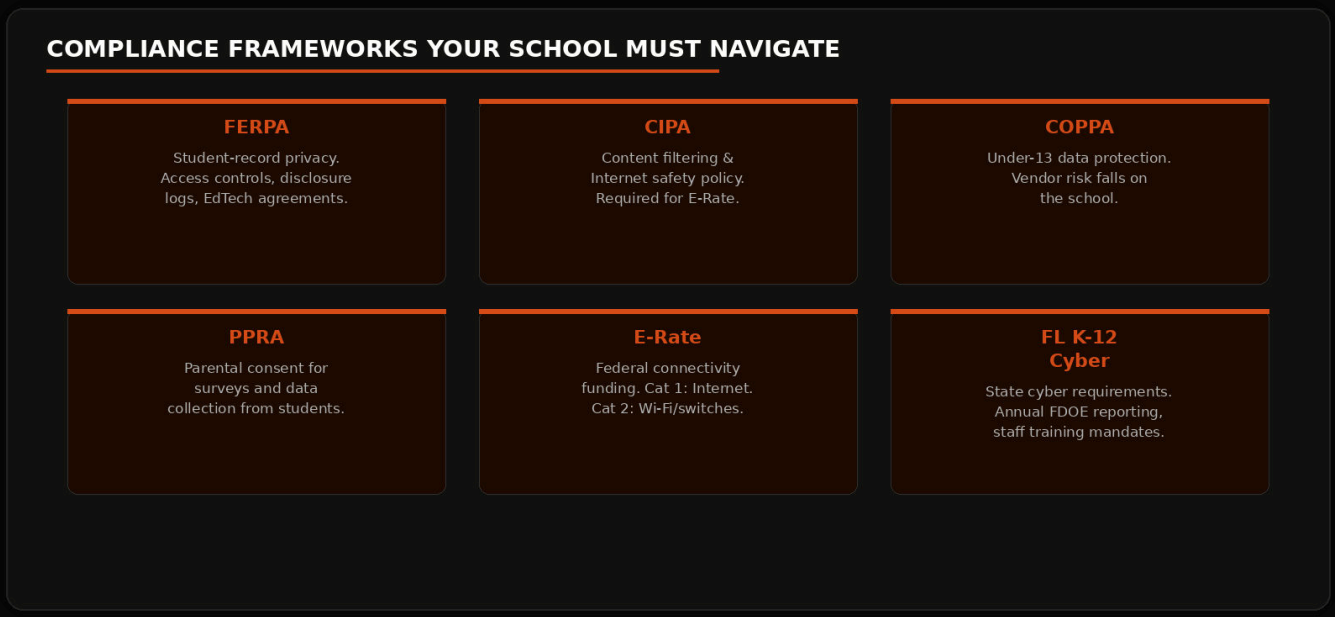
**BOTTOM LINE**

**K-12 is now the most-targeted public sector for ransomware in the U.S. The question isn't if. It's when — and whether your backups will actually restore.**

THE FRAMEWORKS YOUR SCHOOL ACTUALLY HAS TO DEAL WITH

# Compliance isn't optional. It's your job.

Most IT firms know HIPAA and PCI DSS. Far fewer know FERPA, CIPA, and the Florida FDOE reporting requirements that govern how your student data, your content filter, and your federal funding all interact. We do.




## E-RATE — WHAT'S ELIGIBLE

Category 1 funds Internet access and fiber. Category 2 funds internal connections — Wi-Fi, switches, and eligible firewalls (Fortinet is E-Rate eligible). Managed services and ongoing cybersecurity operations run on operating budget, not E-Rate. We help you understand the line and coordinate with your E-Rate consultant.

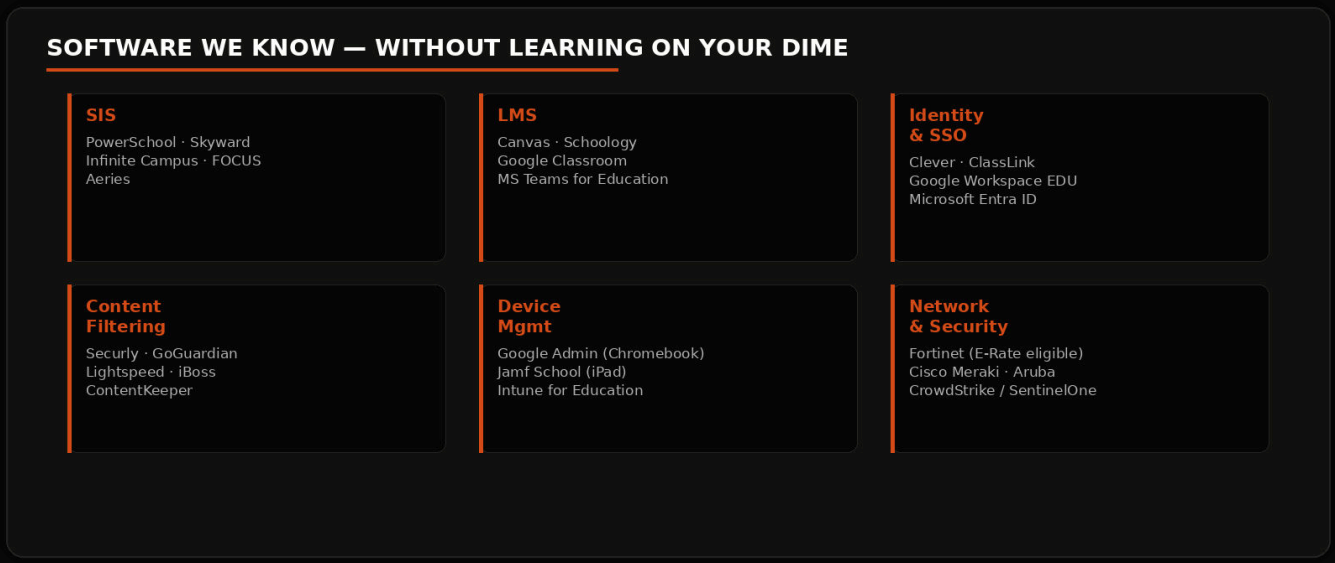
## FERPA BREACH — WHAT TO DO

Treat it as a potential breach until proven otherwise. Preserve audit logs from SIS, LMS, and SSO before they roll off retention. Reconstruct the access path. Draft family communication and FDOE incident report if required. The right time to rehearse this is before the parent email arrives.

WE DON'T LEARN YOUR STACK ON YOUR DIME

# Your platforms. Already familiar.

Most IT firms learn your student information system, LMS, and SSO stack after they're onboarded — on your time and at your expense. We've already worked in the systems South Florida schools run. We know the seams between Microsoft and Google, between Clever and PowerSchool, between Chromebooks and Intune.




The high-leverage work is making the seam between platforms invisible: **real SSO from Clever or ClassLink, Entra federated to Google, off-boarding that fires in both ecosystems at once, and Intune + Google Admin policies that don't contradict each other.**

AN OUNCE OF PREVENTION

# The break-fix conflict of interest.

Under a break-fix model, the IT firm has no incentive to prevent problems. **They're paid by the hour when things stop working.** In a school, that means a frozen Chromebook cart during an assessment is revenue for them — and lost instructional time for your students.

## MANAGED IT SERVICES VS. BREAK-FIX — K-12 EDITION

| | MANAGED IT | BREAK-FIX |
|---|---|---|
| COST | ✓ Flat monthly budget line | ✗ Surprise invoices |
| INCENTIVE | ✓ Prevent problems | ✗ Profit from problems |
| SCHOOL CALENDAR | ✓ Work around testing windows | ✗ Whenever they can |
| FERPA/CIPA | ✓ Compliance built in | ✗ Your problem, not theirs |
| HELP DESK | ✓ Business hours + emergency | ✗ Office hours only |
| E-RATE | ✓ Eligible infrastructure | ✗ No guidance |
| BEST FOR | ✓ Ongoing school operations | ✗ One-off projects only |

RECOMMENDATION

**For ongoing school operations, managed services is the only model that aligns the IT firm's incentives with yours — and with your students.**

INDUSTRY PRICING BENCHMARKS

# What it actually costs.

RRG managed services are priced per device at a flat monthly rate: **$300/month per server, $150/month per PC or workstation, and $5/month per student device** under MDM. These are managed IT prices only — cybersecurity services are priced separately. No surprise invoices, no per-incident fees.

## RRG MANAGED IT — MONTHLY PRICING

Per-device flat rate. Managed IT only — cybersecurity priced separately.

| $300 /month | $150 /month | $5 /month |
|---|---|---|
| **PER SERVER** | **PER PC / WORKSTATION** | **PER DEVICE** |
| SIS hosts, domain controllers, file servers, backup servers | Staff desktops, laptops, admin computers | Chromebooks, iPads, student tablets under MDM |

### WHAT SHOULD BE INCLUDED

Security patches. Antivirus and firewall monitoring. Backup test restores. Spam filtering. Workstation and server health monitoring. Network documentation. Quarterly technology review.

### WHAT'S OFTEN NOT INCLUDED

Hardware. Software licenses. E-Rate filing (coordinate separately). Special projects. After-hours/emergency support. Cybersecurity operations. Ransomware recovery. Get all of this in writing.

GET IN WRITING

**Recovery from a ransomware attack can take hundreds of hours. Confirm IN WRITING who pays for that — you, or them.**

CUSTOMER SERVICE · Q1–Q5

# Get the answers in writing.

How an IT firm handles support determines what happens when a Chromebook cart fails at 8 a.m. on testing day — or when a FERPA question lands in your inbox at 6 p.m.

**Q1 When I have an IT problem, how do I get support?**

You should be able to call, email, or submit a ticket. In a school, a teacher shouldn't have to navigate a portal when a smartboard fails mid-lesson. **We make it easy: call, email, or ticket — any of the three works.**

**Q2 Do you offer after-hours support? What about before school starts?**

Our office hours are 9 a.m.–5:30 p.m. Monday–Friday. **After-hours emergency support is available for critical outages** — the kind that affect an entire campus or a testing window. Ask whether after-hours coverage is included in your monthly fee or billed separately.

**Q3 Do you have a written, guaranteed response time?**

If they don't have it in writing, they can't guarantee it. **Get response time commitments in writing for both business hours and after-hours emergency calls** — and specifically ask what "emergency" is defined as in the contract.

**Q4 Will I have a dedicated point of contact?**

Without one, you'll re-explain your SIS, your Chromebook deployment model, and your testing calendar to whoever picks up. **Our clients get a dedicated account manager who knows your campus, your stack, and your school calendar.**

**Q5 Do you understand the school calendar? Will you push changes during testing windows?**

**We will not push a Wi-Fi cutover the week before FSA testing.** Almost everything non-emergency goes in the summer window or over winter break. We plan twelve months out so the heavy lift happens when students aren't in classrooms.

IT MAINTENANCE · Q6–Q12

# What's actually in the contract.

"All-you-can-eat" contracts almost never are. Know what triggers a surprise invoice before you sign.

**Q6 Do you offer proactive monitoring — or do you wait for us to call?**

Proactive monitoring means catching a failing SIS server before the attendance window closes — not after. If they don't watch constantly, walk away.

**Q7 If we get ransomwared, who pays for recovery?**

Recovery from a serious attack can be hundreds of hours. **Get this in writing.** Also confirm: unlimited help desk, M365 and Google Workspace support, multi-campus coverage, and disaster rebuilds.

**Q8 Is your help desk staffed by people who know school software?**

Ask if they know PowerSchool, Clever, and Google Admin Console. A generic help desk that learns your SIS after onboarding is a liability during peak enrollment and testing periods.

**Q9 How many engineers are on staff?**

One- or two-person firms can't cover a tech being out. **We have a full team of certified engineers, including Fortinet-certified network specialists.** Coverage doesn't disappear when one person is on PTO.

**Q10 Do you document our network?**

Yes — at no extra charge, updated quarterly. Documentation serves as evidence for E-Rate compliance reviews, FDOE audits, and authorizer renewal packages.

**Q11 Do you meet quarterly for a technology review?**

We do. Budget planning, upcoming compliance deadlines, device refresh cycles, E-Rate window timing, and known risks — not a geek-fest.

**Q12 How do I cancel if it isn't working?**

We start every new client with a **3-month trial period.** If you're not satisfied at any point during those 90 days, you can walk away — no penalties, no fines. Our 97% retention is earned, not enforced.

CYBERSECURITY & FERPA · Q13–Q17

# Your IT firm's defense posture.

Student data, ransomware readiness, and FERPA compliance — the questions that separate firms who've worked in K-12 from those who haven't.

### Q13 Do you understand FERPA — not just HIPAA?

FERPA governs student records. Any IT firm working in K-12 must understand access controls, disclosure logs, and EdTech vendor agreements. **Ask them to explain a FERPA incident response process.** If they can't, they haven't done this before.

### Q14 How do you lock down endpoints — especially Chromebooks?

Chromebooks require Google Admin Console policy management. Windows devices need MFA, EDR/MDR, and SIEM logging. **Content filtering satisfying CIPA must be active on every student device, on and off campus.** "We have antivirus" is not an answer.

### Q15 What cyber liability and E&O insurance do you carry?

If their negligence contributes to a FERPA breach or ransomware shutdown, who absorbs the cost — the district, the charter, or them? **RRG carries cyber liability, E&O, and workers' comp insurance. Ask to see the policy.**

### Q16 Who audits YOUR cybersecurity?

Nobody should proofread their own work. **We're audited recurringly by Galactic Advisors.** If a firm tells you their partners audit them, that's not an independent audit.

### Q17 Can you help us pass an FDOE cybersecurity review?

Florida requires annual FDOE cybersecurity reporting and staff training mandates. **We help districts document their posture against Florida K-12 cyber standards** — so you're not scrambling when the deadline arrives.

BACKUPS & DISASTER RECOVERY · Q18–Q21

# The day after the disaster.

Hurricanes happen in South Florida. Ransomware happens in K-12. The question is what your school looks like the next morning — and whether your IT firm can actually rebuild what they say they can.

### Q18 How long until systems are back up after a ransomware attack?

Two phases: **fail-over** (cloud backup goes live, staff can keep working) and **fail-back** (restore to on-premises systems). Critical operations — SIS, email, attendance — should fail over within hours. **Ask specifically about SIS recovery time.** When the SIS is down, the school day effectively stops.

### Q19 Do you do periodic test restores of our backups?

Yes — and we test by actually restoring, not just verifying the backup job completed. **Immutable offsite backups tested by actually restoring from them** is the CISA K-12 cyber guidance standard. Quick test: ask your IT firm to restore three files right now. If they can't do it quickly, you have a problem.

### Q20 If a hurricane hit, how would you keep us operating?

South Florida is in the Atlantic hurricane corridor. Multi-day power and internet outages are part of operating reality for every school district. **Ask how their existing school clients fared during recent hurricanes — and ask to speak to one of them.**

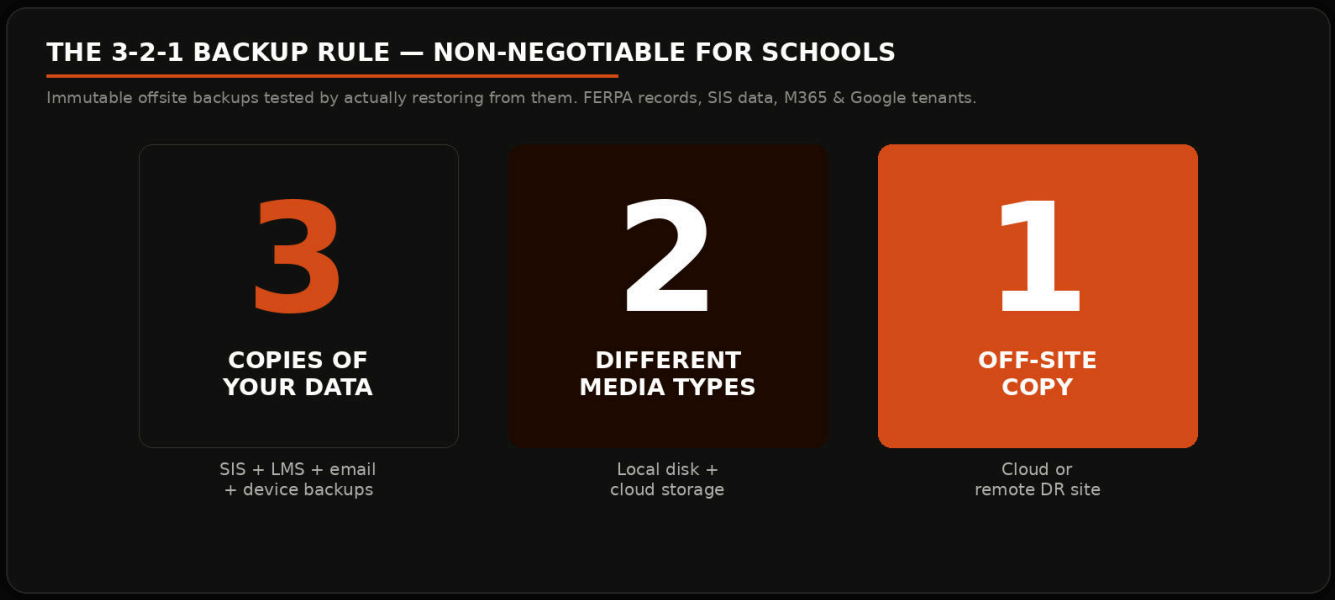
### Q21 Show me your onboarding process.

A real firm has a documented process. For schools, this means: clean credential rotation, secure data transfer, confirmation that no offboarded accounts retain access to student data — and a clear plan for taking over from a predecessor without disrupting the school year.

RANSOMWARE, HURRICANES, AND THE 3-2-1 RULE

# The 3-2-1 rule is non-negotiable for schools.

Student records, attendance data, SIS history, and M365/Google tenant data — these are the records FERPA requires you to protect. **Immutable offsite backups, tested by actually restoring from them,** is not optional. It is the difference between a ransomware incident and a ransomware catastrophe.




We get districts through ransomware readiness in 60-to-90-day phases without taking the help desk offline: **immutable offsite backups, MFA on every adult account (including the superintendent, the board, and the principal who travels), and an incident-response plan with named roles and an annual tabletop drill.**

YOUR NEXT STEP

# 30 minutes.
# No sales pitch.

Call our office and reference this guide for a brief discovery call. We'll cover your Chromebook fleet, classroom Wi-Fi, FERPA exposure, what's actually breaking in your help-desk queue, and your ransomware readiness — honestly. If we're a fit, we'll schedule a full IT Systems Assessment at no charge.

## AFTER OUR FREE DISCOVERY CALL, YOU'LL KNOW:

- **WHERE YOUR FERPA EXPOSURE ACTUALLY IS** — Student data, sharing settings, vendor risk
- **IF CLASSROOM WI-FI WILL HOLD DURING TESTING** — Coverage gaps, AP count, channel planning
- **IF BACKUPS WILL ACTUALLY RESTORE** — SIS, M365, Google tenant tested
- **YOUR RANSOMWARE READINESS SCORE** — MFA gaps, backup status, incident plan
- **E-RATE FUNDING YOU MAY BE LEAVING BEHIND** — Cat 1 & Cat 2 eligibility review

BOOK A DISCOVERY CALL

**(844) 919-8534**

*Reference this guide for your free assessment. rrgnetworks.com/industries/k-12/*

WHY OUR CLIENTS STAY

# Top 7 reasons to outsource to us.

## OUR SERVICE PROMISE TO K-12 SCHOOLS

| Sev1 <15min | 9-5:30 | 24/7 | 100% |
|---|---|---|---|
| SEVERITY 1 RESPONSE TIME | OFFICE HOURS MON-FRI LIVE SUPPORT | SOC SECURITY MONITORING ALL HOURS | NO-SMALL-PRINT SATISFACTION GUARANTEE |

1. **We know the school calendar.**
   We won't push a change during FSA week. Projects go in summer and winter break — planned 12 months out.
2. **No geek-speak.**
   You get answers in plain English. We don't talk down to principals, operations directors, or IT leads.
3. **3-month trial. No lock-in.**
   Try our services for 90 days. If you're not satisfied, walk away — no penalties, no fines.
4. **Projects on time, on budget.**
   Wi-Fi refreshes, SIS cutovers, identity consolidation — what we promised, when we promised it.
5. **No vendor hostage.**
   Full network documentation, written and updated. You can switch firms anytime.
6. **24/7 security monitoring from our SOC.**
   Your network is watched around the clock for threats. Most issues caught and resolved before you notice.
7. **10+ years, 97% client retention.**
   A decade of serving South Florida. Our clients stay because we earn it monthly.

CHOOSE I.T. WISELY.

# Ready to talk?
# Let's start.

A free, 30-minute discovery call for K-12 schools and districts. No obligation. No pitch. Just an honest look at your FERPA exposure, ransomware readiness, Chromebook fleet, and classroom Wi-Fi — from people who already know what FSA week looks like.

---


**(844) 919-8534**

rrgnetworks.com/industries/k-12/

12343 SW 132nd Court · Miami, FL 33186