Look Who’s Talking – Cirrus Technology Solutions

12 May 2026



Q&A | Education Technology

From Connectivity to Confidence

A people-first managed service provider helping schools and growing organisations
scale with confidence, protect what matters, and give their people the tools and support they need to do their best work.

Education IT
Managed IT
Cyber Resilience
Digital Maturity
AI Readiness

Cirrus Technology Solutions

Cirrus is a people-first managed service provider built to support growing businesses and schools that rely on technology to move forward.

“We don’t just manage IT. We help you scale with confidence, protect what

matters,
and give your people the tools and support they need to do their best work.”

Question 01

Looking at the impact of Connect the Classroom so far, what do you feel it has changed most meaningfully for schools beyond simply improving internet speeds?

Connect the Classroom has done more than upgrade bandwidth, it’s shifted the baseline expectation of what “good” looks like.

The meaningful change:

- More active and collaborative learning, reliable connectivity enables real-time collaboration tools, shared documents and multimedia content.
- Lessons have shifted away from passive consumption, more interactive and engaging.
- Improved connectivity can’t fix existing issues which may be masked by the upgrades. In other cases new issues may arise.
- It’s enabled cloud-first adoption at scale, which was previously constrained by unreliable infrastructure.

Connect the Classroom hasn’t solved IT, it’s removed the excuse for poor IT and in turn, improved the student learning experience.

Question 02

As schools move beyond the initial infrastructure uplift, what do you believe leadership teams should now be focusing on most closely?

Focus should be on smooth operations and day-to-day running.

- Assess challenges and risk.
- Prioritise the biggest areas of concern or weakness.
- Build a plan that addresses both and keeps them within your control.

- Set an operational model that underpins your needs and review periodically.
- Ensure you have teacher confidence and buy-in.

The question changes from “Do we have enough bandwidth?” to “Is the experience good enough that nobody has to think about IT at all?”

Question 03

Across the school sector, what are the biggest misunderstandings you still see around “digital maturity” and what it actually means in practice?

A few misunderstandings come up again and again in schools when people talk about “digital maturity”.

The big ones I regularly see:

“We’ve new equipment, so we’re mature.” New doesn’t equal good teaching or consistent use.
“Good Wi-Fi means we’re done.” Connectivity is just the baseline, not maturity.
“Cloud = transformation.” Moving systems doesn’t fix poor workflows or practice.
“IT owns digital maturity.” It’s a whole-school issue, not just an IT metric.
“One-off training solves adoption.” Real maturity needs ongoing confidence and support.
“Students will just ‘get it’.” School systems still need clear design and guidance.
“We have an MSP, so we’re covered.” Many schools are still operating reactively, despite outsourcing.
Digital maturity is actually about control, visibility, and predictability, not tools.

Question 04

In your view, what are the main gaps that still exist between improved connectivity and a truly

resilient, well-managed school IT environment?

Improved connectivity is only one layer. The biggest gaps between “faster internet” and a truly resilient, well-managed school IT environment usually sit elsewhere.

The biggest gaps are operational:

- No single view of the estate, including devices, users and risks.
- Weak identity and access control.
- Poor change management.
- Limited monitoring and alerting.
- Inconsistent support models.
- Ownership and unclear accountability across IT teams and providers.

Connectivity improved the front door, most issues now sit in the back office.

Question 05

What are the most common signs that a school may have stronger infrastructure in place, but still be operating in a reactive or fragile way behind the scenes?

You often see schools that look digitally advanced on paper, fast connectivity, cloud platforms etc. but the tell-tale signs of being reactive and fragile are usually found at an operating level.

What I see:

- Frequent “random” issues no one can explain.
- Heavy reliance on one key IT person or supplier.
- Short fixes instead of root-cause resolution.
- Teachers regularly step in to fix basic tech issues.
- Small changes cause disruption.
- No clear documentation.
- Security tools in place, but no one actively managing them.

Everything works… until it suddenly doesn’t.

Question 06

When schools or trusts begin reviewing their current environment, what are the first areas you believe they should assess most carefully?

When schools or trusts are starting a proper review, the mistake is trying to assess everything equally at once. The most useful starting point is usually the stuff that silently creates operational risk and user frustration.

Start with control and visibility, not tools.

Priority order:

- Identity: who has access to what.
- Device visibility: what exists, what's compliant.
- Support model: who owns outcomes.
- Cyber posture: real vs assumed.
- Change management: how things are updated safely.

Most schools jump to cybersecurity tools before fixing who's actually in control.

Question 07

Many school leaders are not technical specialists. What should heads, school business leaders and trust leaders be asking their IT partner right now?

Non-technical, but powerful questions:

- What are our biggest risks right now, in plain English?
- What's broken or fragile that we might not see?
- If you started again, what would you change first?
- How do you know everything is actually working?
- What does "good" look like for a school like ours and how far are we from it?
- What are you fixing before things go wrong?

- What is the day-to-day experience like for staff and students?
- If you disappeared tomorrow, could someone else run this?

If a partner answers these clearly, in plain language, with evidence, that's confidence. If they drift into jargon, tools, or vague reassurance, that's your signal.

Question 08

How do governance, safeguarding and operational continuity increasingly overlap within a school's digital environment?

In practice, they're increasingly the same conversation because most school risk now sits inside digital systems rather than alongside them.

- Safeguarding depends on controlled access and monitored usage.
- Governance requires auditability and accountability.
- Continuity depends on resilience and recoverability.

Where they overlap most:

- Identity and access management sits at the centre of all three.
- Data integrity and auditability supports safeguarding and governance assurance.
- Resilience of cloud platforms underpins day-to-day teaching continuity.
- Cyber incidents simultaneously affect safety, oversight, and operations.

Schools no longer have separate "IT risk", "safeguarding risk", and "operational risk", they share the same digital backbone.

Question 09

What does a well-supported, low-fragility school IT environment look like in practice?

A well-supported, low-fragility school IT environment is one where technology "just works" for staff and students, and problems are handled before they become visible disruption.

It feels… boring.

- Issues are rare and predictable.
- Changes don’t cause disruption.
- Everything is documented.
- Risks are known and managed.
- Users trust the system.

Fragility shows up as unpredictability. A strong environment removes that unpredictability so teaching time, not IT troubleshooting, is the default.

Question 10

Cyber resilience is now a much bigger part of the conversation. What do schools most need to understand about moving from basic protection to a more proactive and resilient position?

The key shift schools need to understand is that cyber resilience isn’t about preventing every incident, it’s about maintaining learning and operations even when something goes wrong.

Most schools are still at:

- Antivirus.
- Filtering.
- Basic backups.

Resilience means:

- Assuming breach, not preventing it entirely.
- Rapid detection and response.
- Tested recovery processes.
- Strong identity protection, which is now the main attack vector.

Resilience is less about building higher walls, and more about making sure the school can keep functioning even when those walls are tested. Cyber is no longer an IT issue, it’s an operational risk issue.

Question 11

AI is becoming a much more immediate topic for schools. What needs to be in place before schools can confidently and responsibly move further in that direction?

Before schools can move forward confidently with AI, a few foundations really need to be solid first. Without them, AI tends to amplify existing gaps rather than solve them.

- Clear governance and policy.
- Data protection and privacy readiness.
- Security.
- Clean, structured data.
- Clear policies on data usage.
- Strong identity and access controls.
- A clear educational purpose.
- Staff understanding of risks.

Schools don't need to "wait" for AI, but they do need enough governance, literacy, security, and clarity in place so adoption is intentional rather than reactive. Without this, AI just accelerates bad practice.

Question 12

What does "AI readiness" actually mean in practical school terms?

In practical school terms, "AI readiness" isn't about having AI tools already in place, it's about whether a school can adopt, manage, and benefit from AI safely and consistently without disruption.

In reality, it usually breaks down into a few concrete areas:

- **Staff confidence and understanding:** Teachers and leaders don't need to be AI experts, but they do need to understand it.
- **Clear boundaries and policy:** Readiness means having simple, usable

guidance on AI usage.

- **Data protection and safeguarding baked in:** This is often the biggest hidden gap.
- **Curriculum integration:** Readiness here is pedagogical, not technical.
- **Governance clarity:** Without this, adoption becomes uneven or fragile.
- **Culture of professional judgement:** AI-ready schools don't replace judgement with automation. Professional accountability still sits with staff, not tools.

AI readiness means a school is organised enough technically, culturally, and operationally to use AI as a controlled enhancement to teaching and learning, rather than something experimental, fragmented, or risky.

Question 13

Where do you believe AI has the most realistic potential to support schools in the near term, and where should leaders be more cautious?

In the near term, the value of AI in schools is much more practical than transformational. The biggest gains come from reducing workload and improving consistency, rather than replacing teaching.

Cirrus Technology Solutions

A people-first managed service provider helping growing businesses and schools scale with confidence, protect what matters, and support their people.

Visit Cirrus Technology Solutions