9 questions to assess Australian schools' digital strategy

RUCKUS ebook

RUCKUS® COMMSCOPE

DICKER DATA

Introduction

You can't be best-in-class today without A-grade digital technology. With internet connectivity transforming pedagogy, the way students access learning materials and instructors collaborate has dramatically changed.

To keep up, over a third of Australian educators aim to invest in digital technologies within the next 1-3 years. More than 90% agree that the right technologies can help them achieve learning goals and create more accessible, inclusive experiences both in classrooms and distance learning.

But doing so will challenge even the most digitally mature schools and tertiary institutions. Educators already face a raft of challenges, including cybersecurity attacks and the digital divide. New technologies like generative AI and virtual reality, which evolve faster than the most prescient curricula, create as many concerns as they do opportunities for enhanced learning.

How can educational leaders create a digital experience that's safe, seamless and innovative? The answer is simple: **go back to basics**.

Educators who invest in strong digital foundations will be better prepared to meet these new requirements head on. They'll also see improvement in other areas, such as meeting ESG obligations and creating value-added services to set them apart from the growing competition.

We've put together a 9-point assessment to help educators gauge whether their digital infrastructure can provide that safe, seamless, stand-out experience for students and staff alike. Given the stakes, it's a test no learning institution can ignore - so get started today.

1 Does our current Wi-Fi solution capacity and coverage truly meet the school's density and application requirements?

Why it matters

IT administrators for schools and tertiary institutions often adhere to rule of "one access point for every two classrooms". However, today's digital learning environment comes with more than its fair share of exceptions.

From examination halls seating hundreds of students to residential campuses in boarding schools, learning environments come with increasingly dynamic and heterogeneous demands for wireless capacity. Differing considerations around cybersecurity, student safety, and user permissions only add to the complexity of making sure wireless coverage is truly up to speed.

The best strategy for schools is often to go back to basics: auditing existing network solutions to identify subpar performance and unmet requirements in these various areas. For mission-critical applications that means reliable access anytime, anywhere.

2 Can our network meet current and future demand for digital education experiences with rising bandwidth needs?

Why it matters

Demand for bandwidth is rapidly evolving in schools. Advanced learning technologies come with potentially explosive increases in bandwidth consumption – especially when rolled out for hundreds of students at a time – as do digital facilities that rely on the Internet of Things to keep students safe and operations smooth. Those bandwidth demands only grow when you factor in the digital components that are increasingly mandated into core curricula – like national online assessment requirements including NAPLAN and Progressive Achievement Tests (PATs) – as well as the growing push for more accessible remote learning options.

All of this requires substantial amounts of network bandwidth and coverage throughout facilities; guaranteed uptime and reliable connectivity is non-negotiable for schools seeking to provide excellent digital education. That may involve deploying wireless access points with higher range, reliability, and bandwidth; or networks that optimize themselves using AI or automation.

Schools will do well to invest in higher-grade network infrastructure that can scale to meet future demand – even when faced with relatively tight budgets. Future-ready networks typically prove more worthwhile in terms of ROI than adopting lower-cost infrastructure that suffers from early depreciation and requires constant upgrading.

3 Do our network solutions protect students, teachers, and their data?

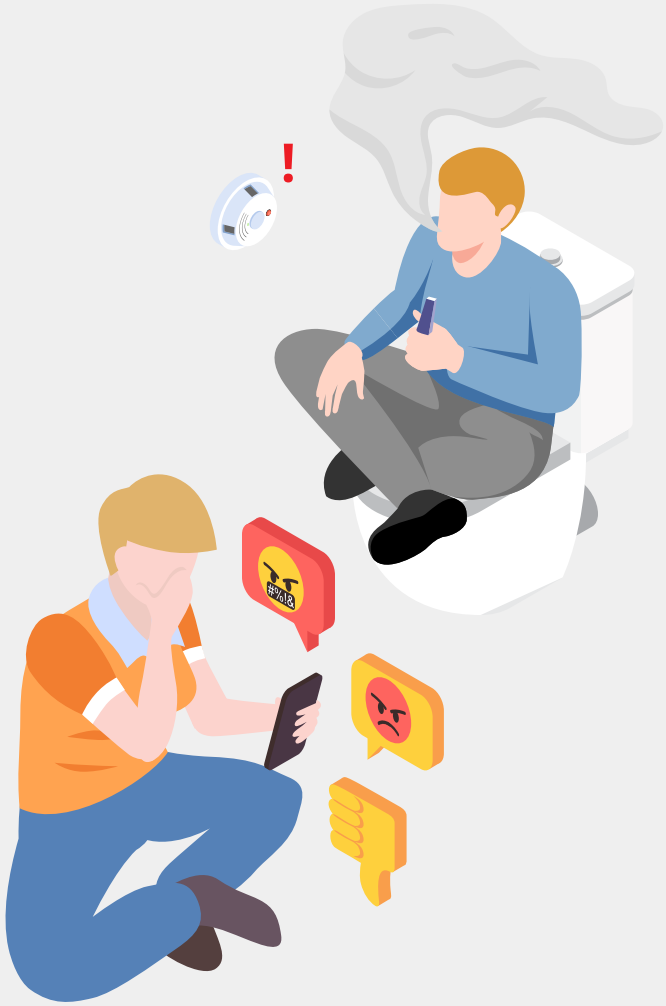
Why it matters

There's no longer any separation between digital security and school safety. On one hand, schools require cyber defences that keep out threats of growing volume and sophistication, particularly those like ransomware which directly threaten sensitive data and operations. On the other hand, they must also filter increasingly diverse forms of content based on user identity – including factors like age or school year – to protect students and uphold their responsibilities to parents.

The best solution to these complex risks is a zero-trust approach to cybersecurity. Zero-trust assumes that all users, devices, and network traffic is untrusted by default – and constantly verifies and checks them at every stage before granting them access to resources on the network.

Achieving zero-trust can be challenging: it requires all network components, from firewalls to Wi-Fi controllers and student management systems, to talk to each other in a way that's automated and secure. With the help of the right network partners, however, it's possible – and arguably the best way to keep schools digitally safe from inside out.

4 Does our network help or hinder the school in fulfilling its duty of care over students' physical welfare?



Why it matters

Fulfilling duty of care continues to pose new challenges, particularly to schools with larger cohorts and lower teacher:student ratios. Staff must not only stay up to date with new risks to student wellbeing like vaping, but also keep an eye out for increasingly subtle challenges like those posed by bullying both online and offline.

Schools with robust networks will find it easier to leverage technology to ensure students' welfare. Internet of Things devices, like smart locks and sensors, can help teachers keep track of more students at any given time and respond where and when they're most needed. Yet even with the most sophisticated devices, school administrators will need to strike a tricky balance between visibility and privacy, particularly in residential facilities like student boarding houses.

The more flexibly a network can adapt to these different use cases, and the more secure the environment in which it hosts sensitive data, the easier it'll be for schools to stay on top of potential risks to students' physical as well as mental wellbeing.

5 Can our network solution reduce our carbon footprint and increase our building's efficiency?

Why it matters

Like other industries, education faces rising scrutiny over its environmental impact. Yet minimising carbon emissions isn't just part of ESG or regulatory obligations – it's also good for business. Smart buildings that use data to run more efficiently have already become the norm in many institutions, which often use automated temperature and lighting controls to minimise consumption during downtime and when staff forget to turn off systems.

Answering this question involves not just different types of Internet of Things devices (like environmental controls and smart lighting), but also networks and platforms that can manage and make sense of the complex data they generate. This allows smart buildings to achieve high levels of readiness for evolving user experience demands, threats from force majeure events like cyber attacks or natural disaster, and the emergence of new technologies and standards.

The right network solutions will craft real-time insight that accounts for indicators of resident wellness, as well as the OpEx efficiency of buildings. Ideally, they'll be backed by vendors who acknowledge their responsibility to environmental and social sustainability in every aspect of product design and management.

These solutions should help administrators create an environment that's both cost-effective and highly livable for residents and staff.

6 Is our network built for cloud-based and distributed learning?

Why it matters

Covid-19 proved the strategic value of remote learning and made it part of educators' lexicon. It also highlighted the need for a tech stack that's purpose-built for flexibility and scalability, allowing educators to deliver curricula with comparable levels of engagement and class inclusion as in-person learning.

The pandemic may be over, but demand for cloud-based and distributed learning only continues to grow. Schools will need ways to effectively manage and integrate diverse device endpoints (like different fleets of laptop or tablet), while also aligning their network functions with other systems like Mobile Device Management (MDM), to ensure a smooth "last mile" for cloud-based learning. They'll also face growing pressure to secure these environments with policy-based user access, data encryption, and automated workflows that protect everyone's data and identity without slowing learning down.

7 Does our network solution come with unified management, complete visibility and analytics over both individual campuses and school groups?

Why it matters

You can't correct what you can't see. In the case of network infrastructure, greater visibility means great ability to tackle complex challenges like shadow IT in the classroom. It also paves the way for more collaborative digital learning experiences that span different campuses, institutions, and geographies – a key point of differentiation that many school groups could benefit from.

This kind of unified management approach involves making the network's control and authentication planes more scalable. Integration between different elements of the network – like the sort achieved when combining RUCKUS' SmartZone Controller and Analytics with Cloudpath's authenticated security solution – also plays a key role. Finally, schools will want to curate different levels of access to network information and analytics, ensuring roles from teachers to group administrators have as much (or as little) control and insight as their duties require.

8 Has our network architecture been designed to support future education outcomes?

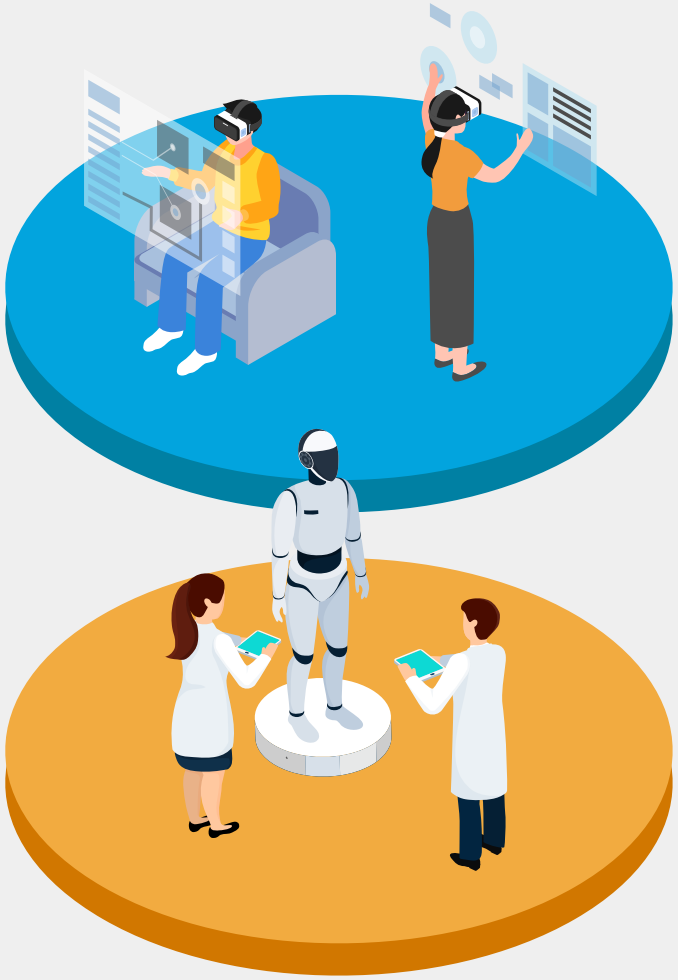
Why it matters

Addressing current network and digital needs is one thing; investing in future-ready infrastructure is another. Yet for educational institutions, achieving future business outcomes will increasingly depend on the strength of their network architecture.

- Digital education technologies like AI and virtual reality will consume exponentially more bandwidth than facilities deal with now.
- Cyber risks continue to grow as the pay-off for successful breaches and hacks increases – along with the regulatory and reputational costs of non-compliance.
- OpEx savings can generate free capital to reinvest in even more efficient operations – creating a virtuous cycle that's crucial when faced with lean budgets and higher competition.

Educators can answer this question with cloud and network solutions that scale without compromising on security or creating excessive complexity.

9 What will stand out to students and parents of the future?



Open question

In an increasingly competitive education system, digital innovation has emerged as a key selling point for both students and parents. Yet those expectations are constantly shifting: what's considered immersive and enriching today can easily become outmoded in a matter of months.

Schools need to constantly refresh digital learning experiences to flourish. They'll need to do the same with teaching digital skills – ensuring students are as up-to-date in their abilities as possible.

Some schools will do best by incorporating digital elements into their existing points of differentiation, like arts or sports programs which already attract students. Others, particularly those with tighter budgets, may consider building digital capacity in a certain niche with long-term relevance, such as AI skills or telepresence experiences. Whatever their strategy, they will need a network foundation that's safe and seamless enough to give them confidence to innovate again and again.

RUCKUS Networks helps you make the grade.

RUCKUS' network solutions tackle the three main challenges for schools' digital strategies: scale, security, and reliability across networks and data.

RELY ON THE WI-FI: thanks to patented technology that supports HD video streaming and other high-bandwidth applications for more students, in all locations from lecture theatres and classrooms to sports fields.

SCALE FAST AND FAR: low-latency, non-blocking architecture provides excellent throughput for the most demanding applications, simplifying network set-up and management, enhancing security, minimising troubleshooting and advanced stacking capabilities that are optimised for key use cases and applications.

SECURE AND SIMPLE: with identity-based policies that secure every connection to your network while minimising friction for guest and new users. Trust powerful safeguards to make sure every connection is secure – including encryption for wireless data in transit, an up-front security posture check before users connect, policy-based access so users get the right level of access, and more.

For more information or assistance with designing your network for students and educators, reach out to **ruckus.presales@dickerdata.com.au**.

Reliable Wi-Fi (indoor & outdoor)

Scalable Switching

Simple Security

Find out more about RUCKUS' solutions at ruckusnetworks.com.

Additional Resources

Case Studies

New Zealand's Ministry of Education taps on Cloudpath and SmartZone to make digital access for students more equitable and secure nationwide.

Leigh Academies Trust reinforces digital learning quality amidst rapid growth with a one-platform approach to network infrastructure.

Ebook

Cloudpath's enrolment and access capabilities are a great fit for the complexity and velocity of primary school environments. **Find out why in this ebook.**

Infosheet

Find out how to **overcome the top IT issues** facing educators today.