BIZCOMMUNITY

3 things school IT teams should prioritise to prepare for our new digital future

By Mandy Duncan

10 Dec 2020

Educational institutions and teachers themselves have come under pressure this year, as the pandemic has pushed them to pivot and adapt to a digital-only world. As schools have now reopened across Europe, and students have reemerged from their virtual classrooms, the digital transformation is by no means complete. Because while the pandemic has created an unprecedented challenge for educational systems worldwide, it has also brought much needed attention to the importance of connectivity and the use of digital technologies for teaching and learning in an open schooling context.

Mandy Duncan, Aruba Country Manager

Moving forwards, schools and universities will be faced with a tricky challenge – caught between financial constraints and the need to future-proof and invest in their networks to support an influx of new technologies. With this in mind, here's what school IT teams should be prioritising right now to prepare for our new digital future.

Setting the right foundations

More than ever, internet access is a necessity for the education sector. Both teachers and students rely on it daily to complete homework, for research purposes, for collaboration, as well as in-class tasks. For those in lockdown, it's also their lifeline and window to the outside world. For the majority of institutions, Covid-19 has meant that learning materials must now be housed online so that students can access it no matter where they are, and similarly teachers' lesson plans are increasingly being stored in the cloud. All of this means that having consistent Wi-Fi access is integral to the learning experience.

However, implementing a Wi-Fi network that spans across campus and provides frictionless connectivity can be difficult. Many schools and universities are still using legacy systems, built to support centralised IT suites. As student Internet of Things (IoT) device usage is on the rise, networks are now being accessed by an explosion of IoT devices at any given time. Now that students are familiar with BYOD usage and personal learning experiences under lockdown, there will be a growing demand for anytime, anywhere network access that supports peer-to-peer collaboration, student-to-staff communication and uninterrupted flexible learning. In order to support this influx of devices, and handle their bandwidth efficiently, IT teams must prioritise integrating enterprise-grade Wi-Fi.

Keep safe

With a fit-for-purpose wireless network in place, schools can unlock the opportunity to digitally transform their classrooms and create truly connected environments. We are seeing an in increased focus on improving operations and efficiencies with IoT-enabled smart spaces that not only promote learning, but also save energy, improve security and save costs. Building automation systems, including energy efficient APs, HVAC, emergency blue light boxes, and smart dormitory door locks make the campus greener and safer.

With contactless experiences high up the agenda, one of the ways to do this is through beacon technology which allows smartphone apps to provide virtual guided tours of facilities for prospective learners and visitors, mapping key landmarks and giving in depth guidance for facilities such as libraries. The same technology is also be applied to warn staff and students of heavy traffic in and around certain areas of a busy school environments, which could be particularly relevant around drop and collect times.

Recent research from HPE Aruba has highlighted the security benefits when edge networking is integrated into the education sector. Asked how they are utilising the Edge today, 49% of IT decision-makers in education cited the use of IoT and location-aware solutions to improve campus safety. With schools and universities now operating in a Covid-19 environment, ensuring the health and safety of students and teachers has never been more important or complex. Deploying IoT solutions at the Edge (45% also said they are using IoT sensors for enhancing student safety) gives administrators greater visibility over how people are moving around campus, which can help to ensure social distancing policies.

Cyber challenges

With an influx of IoT devices, from phones and tablets, to smart speakers and VR, and a cohort that aren’t all aware of security best practices, the network could easily become at risk of intrusion. Not only could this cause a data breach, but more seriously it puts young people at risk of communication from people who may wish to abuse, exploit or bully them.

In order to tackle this issue, schools must implement new tools that go beyond traditional cybersecurity measures, such as AI-based analytics to help identify patterns in typical user behavior and flag anomalies. These kinds of solutions don’t hinder employee creativity, collaboration, or speed as many clunky security systems do. Instead, they provide real-time protection and enable quick responses should a network breach occur.

Conclusion

By implementing a wireless network which can handle multiple devices securely and has the flexibility to adapt and evolve as new technology is added, organisations can set themselves up for success in the future.

With the right technology and a security strategy in place that allows educators to innovate without fear of cyber threats, there is huge potential for educational institutions to become efficient, productive and inspiring digital workplaces – all while navigating the new normal.

ABOUT THE AUTHOR

Mandy Duncan is Country Manager for Aruba