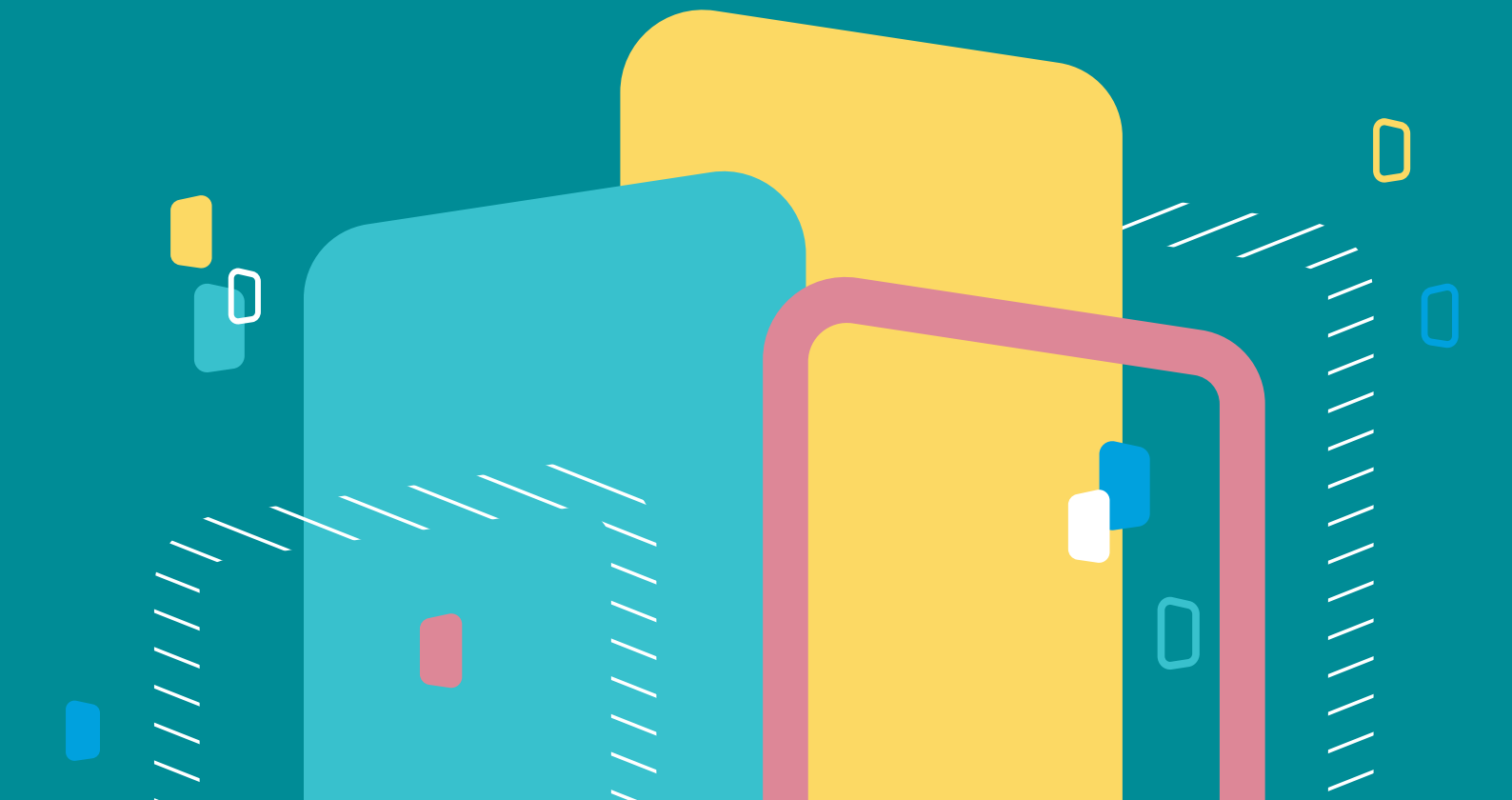
BenQ Education

Shape the Future of Learning

Securing Classroom Technology

Cyber Security Considerations for Education Leaders

Author: Abid Patel, Founder & Managing Director, #ITjustworks



Executive Summary

Schools are increasingly reliant on digital technology to deliver learning, safeguard pupils and operate effectively. With that reliance comes responsibility. While much attention has been given to securing laptops, servers and cloud platforms, classroom technology itself is often overlooked. Interactive whiteboards and panels now sit at the centre of teaching and learning, yet they are rarely considered through the same risk, data protection, and accountability lens as other IT systems. For education leaders, this creates a growing blind spot, one that has implications not just for cyber security, but for governance, compliance and trust.

Modern interactive panels are no longer passive display devices. They are fully-fledged computing endpoints, often running Android operating systems, connected directly to school networks, used daily by staff and pupils, and in many cases handling authentication, user data, and internet access. Yet in many schools, these devices are not managed, patched or secured in the same way as laptops or desktops.

Increasingly, schools and trusts are expected to plan for cyber incidents on a 'when, not if' basis. This makes detection, containment and recovery just as important as prevention, particularly for always-connected classroom devices.

This white paper explores why interactive displays represent a growing and underestimated cyber security risk in education, particularly in environments where equipment remains in use well beyond its supported lifespan. It examines what IT professionals and school leaders should expect from secure interactive display solutions, and how BenQ's approach addresses these needs through long-term Android security support, identity-based access, centralised device management, in-house platform development and transparent data residency, all without ongoing subscription costs.

The goal is simple: to help schools reduce risk, improve confidence in their classroom technology, and treat it as a core part of their cyber security strategy.

The Changing Role of Interactive Displays in Schools

For many years, interactive whiteboards and projectors were largely seen as presentation tools. They displayed content from a connected computer, but they themselves were not intelligent devices. As a result, they were rarely considered part of the school's attack surface.

That picture has now changed completely. Today's interactive displays are effectively computers mounted on classroom walls. Most run Android operating systems, include built-in browsers, microphones, and cameras, support wireless casting, connect directly to internal networks, and allow users to sign in, store files and access cloud services. In practice, they function as network connected IoT (Internet of Things) endpoints, meaning they are devices that connect to the school network, run software, and exchange data, much like any other computer.

Despite this shift, the perception of interactive panels has not always kept pace with reality. While schools rightly focus on refreshing laptops, managing mobile devices and patching servers, displays are often left running for many years with little scrutiny. They are commonly misunderstood as just screens, when in fact they are unmanaged endpoints with significant privileges.

This misunderstanding is rarely intentional. It is often the result of stretched budgets, long refresh cycles and the assumption that classroom displays are low risk. However, as cyber threats in education continue to rise, these assumptions no longer hold. If a school would not deploy an unmanaged Android tablet with full network access into every classroom, it should pause and consider why an unmanaged interactive panel is acceptable.

Cyber Security Risks Associated with Interactive Boards

When interactive panels are not treated as first-class IT assets, several risks emerge. Individually, these risks may seem manageable, but collectively, they can significantly weaken a school's overall security posture.

One of the most common issues is unsupported or no longer updated operating systems. Panels may continue to function long after their software support has ended, creating a false sense of safety. Without regular security patches, known vulnerabilities remain exposed and can persist unnoticed for extended periods.

Schools are already familiar with the risks associated with operating system end of life. Windows 7 reached end of support following years of clear communication from vendors and government guidance. More recently, Windows 10 followed the same path. These milestones were highly visible, often accompanied by national campaigns, funding considerations and explicit risk warnings.

By contrast, the end of support for interactive displays and IoT-style devices has not been communicated with the same clarity or prominence. There are no national alerts, no consistent lifecycle messaging, and no widespread understanding that a classroom display may be running an unsupported operating system. As a result, many schools continue to operate panels that are no longer receiving security updates, without realising the risk this presents.

Another risk relates to authentication and access control. In many schools, panels are shared devices. Without proper identity-based access, this can lead to shared logins, weak passwords or accounts that are never logged out. Credentials can be cached on the device, files can be left behind, and there is little accountability for who accessed what and when.

Wireless casting and screen sharing introduce further complexity. While incredibly useful for teaching and learning, poorly secured casting features can allow unauthorised devices to connect, potentially exposing sensitive content or creating disruption. Without central control, it becomes difficult for IT teams to balance usability with security.

USB ports and peripheral access also present risks. Unrestricted access can enable data exfiltration or introduce malware. On devices that are assumed to be just screens, these ports are often left open by default.

There is also the question of data. Panels may store cached files, user profiles or application data locally. Without proper separation between users and automated session controls, this can lead to accidental data leakage, particularly in environments where multiple staff share the same classroom.

Perhaps most concerning is the role these devices can play in a wider attack. An unpatched, unmanaged panel connected to a trusted internal network can act as a stepping stone for lateral movement. Attackers look for the weakest link, and in many schools, that link is not the server or the firewall, but the forgotten device on the wall.

Incident response and recovery capability is another often overlooked consideration. As schools and trusts increasingly plan for cyber incidents on a “when, not if” basis, the ability to quickly contain risk becomes critical. Centralised and remote visibility and control, including the ability to immediately restrict access, isolate devices and review activity, can significantly reduce impact and support effective investigation and recovery.

End of Life Equipment and the Hidden Risk in Classrooms

The challenge of outdated equipment is not new in education. Many schools are managing mixed estates, with devices of varying ages and capabilities. Budget pressures have extended refresh cycles, and IT teams are often forced to prioritise the most visible or critical systems. When discussions about end-of-life equipment arise, attention usually turns to laptops, desktops and servers. Interactive panels rarely feature in these conversations.

The problem is that because panels are physically robust and continue to function as displays long after their software support has ended, they often remain in classrooms well beyond their secure lifespan. A panel may still turn on, still show content and still appear to work, even though it is no longer receiving security updates or manufacturer support.

An unsupported network-connected device presents the same level of risk as an unpatched computer. The difference is that it is less likely to be noticed, less likely to be audited, and less likely to be included in incident response planning. Recognising interactive panels as computing devices, with defined lifecycles and support expectations, is a critical step in reducing this hidden risk.

What IT Professionals Actually Need from Interactive Panel Security

From the perspective of Network Managers, Heads of IT and IT Directors, security is not about individual features. It is about consistency, predictability and control.

First and foremost, IT teams need centralised management This means having the ability to see all devices, apply policies consistently, manage updates and respond quickly to issues without physically visiting every classroom. It also includes monitoring device health and status, viewing dashboards showing update compliance, and accessing

analytics that support operational decision-making and audit readiness.

Identity-based access is equally important. Shared credentials increase risk and undermine accountability. Secure solutions should integrate with existing identity providers and apply authentication at the device level, not just within individual applications. Strong authentication must be balanced with classroom reality. Solutions that are theoretically secure but impractical to use will cause staff frustration and will inevitably be bypassed. Technologies such as NFC based authentication offer a way to introduce strong, multi factor security without impacting teaching and learning.

Long-term support and patching are non-negotiable. Devices should receive regular security updates for a clearly defined period. This should be part of the core offering, not an optional add-on.

Transparency matters too. School and trust leaders, including Data Protection Officers and data protection teams, need clarity around how data is handled, where it is stored, and which legal and regulatory frameworks apply. Increasingly, leadership teams are asking not just whether a platform is GDPR-compliant, but whether its data residency, governance and accountability align with their organisational risk appetite and statutory responsibilities.

Schools need solutions that are sustainable. Hidden subscriptions, fragmented platforms and complex licensing models create long-term challenges. Security should simplify life, not add another system to manage.

A Security-Led Approach to Interactive Displays

BenQ's approach to interactive panel security is built around the understanding that these devices are part of the school's wider IT estate, not standalone tools.

A key differentiator in BenQ's approach is its end-to-end ownership of interactive display technology. Rather than relying on a collection of third-party or bolt-on systems, BenQ designs and develops its hardware, operating environment and supporting cloud platforms as a single, integrated ecosystem. For education IT leaders, this results in tighter alignment between hardware and software, more predictable behaviour across devices, clearer accountability, and more effective long-term support without reliance on multiple vendors.

This integrated model also has important security implications. Supply chain and firmware integrity are increasingly critical considerations in education, particularly where responsibility for updates, vulnerabilities or remediation can become fragmented. By maintaining control across the full technology stack, security controls can be embedded directly at device level rather than layered on afterwards. This reduces dependency risk, improves device trust, and ensures that security is applied consistently throughout the lifecycle of the panel.

At the centre of this approach is a suite of cloud-based management and security platforms that are provided without subscription fees.

BenQ Device Management Software (DMS) allows IT teams to centrally manage panels across their organisation. Through a single console, administrators can remotely monitor device status, deploy firmware and application updates over-the-air, install or remove apps, determine power-on and power-off schedules, and manage sleep states to support energy efficiency.

DMS also provides dashboards and analytics that give visibility into device health, usage and update compliance, supporting both day-to-day operations and longer-term planning.

Security controls include device locking to an organisation, application allowlisting and blocklisting, port control through authentication modes, and certificate installation at root level to align panels with existing network security models. Automatic application updates ensure that software remains current, and full device control reduces the need for onsite intervention.

Additional features, such as air quality monitoring, provide wider safeguarding and wellbeing benefits beyond pure IT management.

BenQ Account Management System (AMS) provides cloud-based access and profile management for users of interactive panels. AMS enables personalised sign in, isolated user profiles with secure storage partitions, and seamless access to cloud services linked to a user's existing identity provider. This reduces the need for shared credentials and supports clearer audit trails for access and usage.

AMS also supports secure authentication flows, selective resource provisioning per user role, integration with directory services, and consistent profile roaming across compatible devices. By managing access and user segmentation at the cloud level, AMS reduces the risk of data exposure across shared devices, simplifies lifecycle management of user accounts, and aligns interactive panels with broader identity and access management strategies.

BenQ X-Sign is a digital signage platform that enables centralised creation, scheduling and distribution of content across managed displays. X-Sign supports secure template-based signage workflows, allowing schools to broadcast announcements, schedules and other messaging without reliance on USB drives or unmanaged media.

X-Sign's content management capabilities include remote deployment of multimedia, group-based display targeting, and time-based scheduling. By separating signage workflows from interactive panel usage, X-Sign helps reduce risk associated with unmanaged content distribution and supports consistent communication across school and trust environments.

Together, these platforms allow interactive panels to be managed and secured in line with other endpoints, without adding complexity or cost.

Different Approaches to Interactive Panel Security

Not all interactive panel management solutions take the same approach to security, and schools are not always aware of the differences until challenges arise. Some platforms rely on ongoing subscriptions for core security features. While this may be appropriate in some contexts, it introduces long-term financial and operational considerations. If subscriptions lapse, schools may find themselves with reduced functionality or unsupported devices. In other cases, identity integration is limited or applied only at application level rather than device level.

Data residency is another area where clarity is essential. While many platforms state that they are GDPR compliant, this does not automatically mean that data resides within the European Union. Data may be processed or stored in jurisdictions where legal oversight, state access or geopolitical considerations raise valid questions for UK schools. A security-led approach requires transparency. Schools need to understand not just whether a system is compliant, but how and where their data is handled. BenQ's platforms store data in Frankfurt, Germany, operate within EU data protection frameworks, and are supported by teams in the UK and Europe. This clarity reduces uncertainty and support informed decision-making.

Cyber Security in the Wider Education Context

Interactive panels do not exist in isolation. They are part of a broader digital ecosystem that includes cloud platforms, mobile devices, networks and users. Education remains an attractive target for cyber attacks. Schools hold large volumes of sensitive data, often operate with limited resources, and rely heavily on availability. Disruption has real-world consequences for safeguarding and continuity. Increasingly, schools and trusts are recognising that cyber security is safeguarding, as failures in digital systems can directly affect their ability to protect pupils, maintain oversight and meet their duty of care.

As digital technology becomes embedded in physical learning spaces, these safeguarding responsibilities extend beyond data and systems into how classroom technology is accessed, controlled and used day-to-day. Interactive panels are often shared, always accessible and used by multiple groups throughout the day, including during unsupervised periods such as clubs, lettings, cover lessons or after-school use. Modern interactive panels commonly include microphones, cameras and local storage, which can introduce safeguarding concerns if appropriate controls are not in place.

From a safeguarding and governance perspective, school and trust leaders need confidence that classroom technology always supports appropriate use. This includes time-based access controls, differentiated permissions for staff and pupils, the ability to restrict or disable hardware features where required, and visibility over when and how devices are accessed.

At the same time, staff are under significant workload pressures. Security measures that add friction or complexity are unlikely to be adopted consistently. This is why culture matters as much as technology. When security expectations align with everyday classroom practice, they are more likely to be followed reliably and responsibly, supporting both safeguarding and wider cyber resilience.

Reducing risk is not about eliminating every vulnerability. It is about removing obvious weaknesses and ensuring that no part of the environment is forgotten.

Aligning with DfE Digital and Cyber Security Standards for Schools

The Department for Education has set out clear Digital and Cyber Security Standards for schools and colleges. These standards define the baseline expectations for a secure educational environment, and interactive panels sit squarely within their scope. Several areas of the standards are directly relevant to classroom display technology.

Software updates and support:
The DfE expects all devices to be supported and regularly patched. An interactive panel running an operating system that is no longer receiving security updates presents the same risk as an unsupported laptop or server and is a clear gap against this expectation.

Identity and access management:
The standards emphasise controlled access to systems and services. Shared logins on classroom panels undermine this principle, making it difficult to demonstrate accountability, audit access, or protect sensitive staff and pupil data.

Network security:
Protecting the school network from unauthorised access is a core requirement. An unmanaged interactive panel connected to the internal network can act as an entry point for lateral movement, increasing overall organisational risk.

Viewing interactive panels through the lens of the DfE standards reinforces a simple message. These devices should be treated as part of the school's core IT estate, subject to the same expectations around lifecycle management, access control and network protection as any other connected system.

Cyber Essentials is increasingly used by trusts and local authorities as a baseline assurance framework when assessing cyber risk and sits alongside the DfE standards as a useful organisational reference point. While no framework guarantees security, its core principles reflect practical expectations around secure configuration, access control and protection against common threats. When applied to classroom technology, this reinforces the importance of managing applications, controlling device access and ensuring systems remain supported and maintained throughout their lifecycle.

Communicating Cyber Security to Educators

For security messaging to resonate in education, it must be grounded in reality. Educators do not need fear-based messaging or abstract threats. They need clear explanations of risk, practical solutions and reassurance that security does not have to be complicated.

Effective communication should focus on responsibility and control. Interactive panels should be presented as part of the school's safeguarding and duty of care, not just as teaching tools. Messaging should acknowledge the pressures schools face and offer solutions that fit within existing workflows. Transparency builds trust. Being clear about what a system does, how it is supported, and how data is protected creates confidence across leadership teams.

Above all, security should be positioned as an enabler. When done well, it reduces workload, increases confidence and supports better outcomes for staff and pupils.

Conclusion

Interactive panels are now among the most widely deployed computing devices in schools, yet they remain one of the least scrutinised from a cyber security and governance perspective. As classrooms become increasingly digital, these devices sit at the intersection of teaching, data access and network connectivity, making them impossible to ignore in any serious conversation about risk and accountability.

For education leaders, the challenge is not simply technical. It is strategic. Outdated operating systems, unmanaged access and unclear data handling practices introduce risks that extend beyond IT teams and into safeguarding, compliance and organisational trust. As with laptops, servers and cloud platforms, interactive panels require clear

ownership, defined lifecycles and consistent security expectations. Treating classroom technology as part of the core IT estate is no longer optional. Schools and trusts that take a proactive approach, embedding identity-based access, centralised management and long-term support into their interactive display strategy, place themselves in a far stronger position to reduce risk, demonstrate compliance and build confidence across leadership teams, staff and communities.

BenQ's security led approach reflects this reality. Through in-house platform development, long-term Android security support, transparent EU-based data residency and subscription-free management tools, BenQ provides a model that aligns classroom technology with modern cyber security and governance expectations.

Ultimately, the question for schools is not whether interactive panels should be secured, but whether they are prepared to view classroom technology through the same risk, data and accountability lens as every other system their organisation depends on. Those that do will be better equipped not just to respond to threats, but to lead confidently in an increasingly complex digital landscape.

BenQ Education

Shape the Future of Learning

Explore BenQ Education

www.BenQ.co.uk/Education