Linewize Insights

The risks of unmanaged devices

What the risks are, how to reduce them, and the options open to your school.

If we can't control the device, can we still control the learning?



linewize.io

Linewize by Qoria

Before you start

A discussion paper for school leaders and IT teams in Asia Pacific, including British international schools, running Bring Your Own Device (BYOD) programmes.

The risk in your school isn't who owns the device. It's who controls it.

Contents

01	Introduction
02	The problem was never ownership
03	Admin rights: the decision that undoes every other decision
04	Unmanaged devices cost a lot more than you think...
05	The rules keep changing
06	KCSIE: a UK standard in a BYOD world
07	Privacy, trust and parent choice
08	The best you can do. Is it enough?
09	You may already have most of what you need
10	Where to start
A	Appendix: for IT teams



01

Introduction

Most schools never chose to run an unmanaged device programme. They arrived at one.

BYOD had its place, and in many schools it still does. As learning moved online, schools wanted a device in every child's hands. Someone had to pay for that. Government funding needs a long-term commitment that outlasts changes of government, and in much of the region it never came.

So BYOD often started informally. If a child had a laptop at home, they were welcome to bring it. It helped, and it cost the school nothing. Over time, "welcome to bring one" became "expected to bring one". The school avoided the hidden costs of owning a fleet: buying, managing, supporting, insuring and replacing it. Families paid, technology reached every classroom, and schools met a real need without waiting on anyone else.

But when the cost moved to families, control of the device moved with it. Nobody decided that. It happened because control followed the money.

Control followed the money.

When BYOD began, that didn't matter much. The environment was controlled. A student's laptop joined the school network, and the school's filter did the rest. A laptop was still a bit of a privilege, and most students didn't carry a phone with its own data. In that world, an unmanaged device was manageable.

Then two things changed.

The first is how the device is used. It moved from the edge of learning to the centre of the school day. It is also the student's personal device, holding their games, films, social media and friends. We ask them to ignore all of that for six hours a day.

The second is what students can do with it. A hotspot is in almost every pocket. VPNs are sold to families as privacy tools. AI will help a student write code to get around a filter in minutes. Many of the controls schools rely on were built for a world that no longer exists.

The devices changed. The tools changed. The way students use them changed. Has the way schools keep students safe and focused in class changed as much? In most schools, the honest answer is no.

That's why schools with BYOD programmes everywhere ask us the same questions:

How do we stop VPNs?

How do we stop hotspots?

How do we stop games in class?

How do we keep students focused on learning?

Many schools would say they run BYOD well. Most have also come to accept these problems as the price of running it. But these problems aren't the sign of a badly run programme. Even the best-run unmanaged programmes have them, because they're built into the model. Better management won't fix them. Only control will.

So the question for every BYOD school is no longer whether BYOD works. It's this:

If we can't control the device, can we still control the learning?

This paper argues that BYOD isn't the problem. Losing control of the device is. Who holds that control, and how a school takes it back, is what the rest of this paper is about.

02

The problem was never ownership

In the controlled world BYOD was built for, the network did the work, so it hardly mattered who administered the device. Now that a student can step off the network whenever they like, it matters more than anything else.

Debate in schools usually splits along one line: family-owned or school-owned devices. Both are 1:1 programmes, with a device for every student. The line that matters runs between managed and unmanaged, and that comes down to who holds administrative control.

	Unmanaged BYOD	Managed BYOD	Managed school-provided devices
Who owns the device	The family	The family	The school, often funded through fees or a device levy
Who holds administrative control	The student, by default	The school, by agreement with the family	The school
Student admin rights	Full	Removed	Removed
Filtering	Network only. Stops when the student leaves the school network	On the device. Travels with the student and can't be removed	On the device. Travels with the student and can't be removed
VPNs, proxies and hotspots	The student's choice	Blocked on the device	Blocked on the device
Classroom control	Teachers can ask students to close their screens	Teacher-led, in real time	Teacher-led, in real time
Consistency in the classroom	Every device is different	One school-specified platform, same controls	Identical devices and setup
Technical support	Every device is a special case	Standard configuration, remote fix	One fleet, one process
Purchasing	Each family buys alone	Each family buys, within school requirements	Centralised, with the school's buying power
Evidence after an incident	Whatever the firewall happened to log	A student-level record	A student-level record

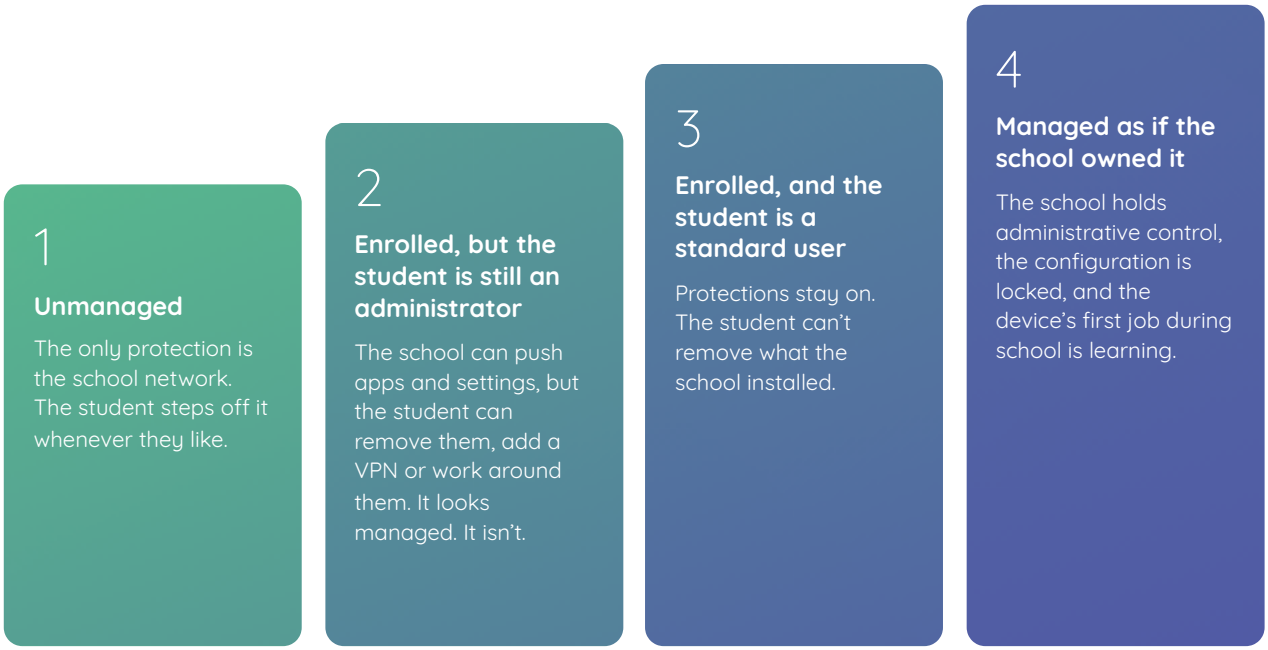
Look at what changes between the first two columns. The hardware doesn't change. The funding model doesn't change. Families still buy the device and still own it. Nobody has to find capital for a fleet, or write off the devices already in student bags.

What changes is administration, and everything that sits downstream of it. That is a policy decision and a conversation with families far more than it is a procurement decision.

> Moving from column one to column two costs no new hardware. It costs a decision.

Managed means more than enrolled

When we say managed, we don't just mean enrolled in a device management system. Management comes in levels, and the gaps sit between them.



No school can guarantee a student's safety online, because some students will always be working to get around protections. But each level up removes another way around them. The higher the level, the more confidently a school can say it is doing everything it can, and the more of Keeping Children Safe in Education (KCSIE) it can actually evidence.

Choose one platform

Managed BYOD doesn't mean any device will do. The school can still specify the platform: for example, Windows or Mac, not a mix. Either platform works well online. But students and teachers are fastest on the platform they know, and the most basic navigation trips people up when they switch. One platform means one set of instructions, one support process and one lesson plan that works on every screen.

The case for school-provided devices

Control follows the money, so bring the money back. Managed BYOD closes most of the safety gap. Some schools go a step further and provide the device themselves, without finding new capital to do it. Instead of each family buying its own laptop, families pay the school what they would have spent anyway, and the school supplies the same managed device to every student. In a fee-paying school, that cost can sit inside the existing fee structure.

The benefits go well beyond safety.

- **Centralised purchasing power.** One order for a whole cohort buys better pricing, warranty and repair terms than hundreds of families buying alone.
- **Identical devices in every classroom.** Teachers know exactly what every device can do, so lessons run the same way for every student and nobody waits while one laptop is fixed.
- **Known, consistent protection.** The school knows how every device is configured and protected, because it set them all up the same way.
- **Equity you can see.** No child is singled out by the laptop they carry, and no child's protection depends on what their family can afford.
- **One fleet for IT.** One build, one process, one set of fixes.
- **A device that's for learning.** Its first job is learning, not entertainment with schoolwork added on.

> We ask students to wear a uniform. Why don't we ask the same of their devices?



03

Admin rights: the decision that undoes every other decision

On an unmanaged BYOD device, the student is usually the administrator. Not because anyone chose that. Because it is the default.

That one fact sits underneath almost every other risk in this paper. A student with administrator rights on the device they bring to school can:

- Uninstall the filtering or safety software the school asked them to install
- Add a VPN, a proxy or a portable browser in under a minute
- Create a second account the school has never seen
- Turn off updates and security protection
- Install anything at all, from anywhere at all

Everything else the school does sits on top of that. The acceptable use policy, the filter, the wellbeing programme, the parent information evening. All of it assumes the controls underneath are still there in period five.

If a student can remove a control, the control is optional. And a control that is optional isn't really a control. It's a request.

This is not a comment on student character. Most students never try. It is a comment on defaults. Give any year group a device where the safety software can be switched off, and sooner or later one student will work it out. Then the rest will know how.

> If the student is the administrator, the student decides whether they're safe. No filter, no policy and no software the school installs can override that.

Admin access is what attackers look for first

Gaining administrator access is one of the most common goals in a cyber attack, because it unlocks everything else on the device. Elevation of privilege, the type of flaw that turns a standard user into an administrator, made up 40% of the vulnerabilities Microsoft disclosed in 2025. Critical vulnerabilities doubled year on year, from 78 to 157. On an unmanaged student device, that access has already been handed over.[1]

This is settled ground in security guidance

The CIS Critical Security Controls, one of the most widely used security frameworks in the world, are clear: administrator access should be kept to dedicated admin accounts, and everyday activity should happen on a standard account. CIS treats this as one of the essential basics every organisation should have in place. It is not an advanced measure. It is a baseline.[2]

You can't secure what you can't see being installed

With admin rights, a student can install anything, from anywhere. Most of it will be harmless: games, browser extensions, apps a friend recommended. Some of it won't be. Free downloads, cracked software and "unblocker" tools are a common way for malware to reach a device. And an infected laptop doesn't stay a personal problem when it joins the school network every morning.

For the school, the cost shows up in learning. A device fails in the middle of an assessment, coursework is lost, or a lesson is spent on IT rather than the subject. A managed device only runs what the school has approved, so it's ready to learn on every day.

"Can students uninstall your software?"

It's the question every BYOD school asks. On a device where the student is the administrator, the honest answer from any vendor is yes, or close to it. An administrator can uninstall software, change settings, add a VPN, edit system files or route around it in more ways than anyone can list. Making software harder to remove only moves the problem, and it causes new ones on devices that are managed properly. Tougher software isn't the answer. Removing the student's admin rights is.

The obvious objection, and a straight answer

"We can't take admin rights away from a laptop a family paid for."

Schools can, and many do. There's no technical barrier. It's a policy decision, made once and written into the BYOD agreement.

Who owns the device doesn't matter. What it's for does. If a device is used for learning, the school manages it fully for as long as it's used for learning. The family keeps ownership. When the student leaves, or the family replaces the laptop, the school releases it, and it's theirs to do with as they wish.

Making a parent the administrator sounds like a fair compromise. It doesn't work. In most homes, the IT support is the student. Many students already know the admin password, or set it up themselves. And a parent can't push an update, fix a setting or restore a safeguard in the middle of the school day.

An arrangement that works for 25 students can't work for 2,500, let alone 25,000. There is no middle ground. Either the school manages the device, or the student does.

In most homes, the IT support is the student.

[1] BeyondTrust, Microsoft Vulnerabilities Report, 13th edition (2026)
[2] Center for Internet Security, CIS Critical Security Controls v8.1





04

Unmanaged devices cost a lot more than you think...

When devices aren't centrally managed, the effects reach well beyond the IT office. They are rarely visible day to day. Most schools only see them clearly when something goes wrong.

You cannot safeguard what you cannot see

Duty of care doesn't shrink because the device is privately owned.

A school's safeguarding obligation follows the student and the learning, not the asset register. If a child is harmed online during the school day, on a device the school asked them to bring, "we had no visibility" is a hard answer to give a parent, a board or a regulator. Unmanaged devices leave schools accountable for outcomes they have little ability to see.

That doesn't mean schools need unrestricted access to students' personal lives. It means knowing where their visibility begins and ends, and being confident it is enough to meet their responsibilities.

Nearly 70%

of children aged 8 to 18 worldwide had at least one online risk in the past year.

DQ Institute, Child Online Safety Index 2023

69%

of teens experienced an online risk in the past year. Only 41% of parents feel very prepared to talk about it.

Microsoft Global Online Safety Survey 2025

55%

of children surveyed in the Philippines did not know how to report harmful content on social media.

Disrupting Harm in the Philippines, UNICEF, ECPAT and INTERPOL, 2022

Bypass stops being an exception and becomes the norm

Network filtering protects the network. Students stopped depending on the network years ago.

A personal hotspot, a free VPN or a portable browser on a USB stick puts a student outside the filter without them leaving the classroom. On a managed device, each of those can be blocked at the source. On an unmanaged one it is a two-minute job, and no network filter can stop it, because the student has already left the network. The method travels through a year group in days.

AI makes this faster. Most AI tools will refuse a direct request to get around a school filter, but they can still explain the techniques, answer more specific questions about proxies and help students write or fix the code (Linewize, May 2026).

Who decides whether a student is safe?

On an unmanaged device, one person decides whether the safeguards stay on: the student.

The tools for switching them off are now easy to find, and many are presented as safety tools. In a 2025 survey of UK children aged 8 to 17, the most common reason young people gave for using a VPN was privacy and staying safe online. Among those who used one, 16% said they had used it to get around school wifi blocks and monitoring (Childnet, 2025).

That puts a big decision on a young person. A study of more than 5,000 people across 11 countries, including China, India, the Philippines and Thailand, found that sensation seeking rises through adolescence and peaks at 19, while self-regulation keeps developing until the mid-20s (Steinberg et al., 2018). An earlier study found that teenagers aged 16 and under think less about the future than adults do, and lean more towards immediate rewards (Steinberg et al., 2009).

None of this is a criticism of students. It's how adolescence works, everywhere. But it means an unmanaged device hands the most important safety decision to young people at exactly the age when it's hardest to put the long term ahead of the moment.

> On an unmanaged device, the student decides whether they're safe. We're asking them to make that call at the age when it's hardest to.

What we're really asking of students

Think about what an unmanaged device asks of a student. Here is the device that holds your games, your films, your social media and your friends. Now open it in class, connect to the school network and use it only for schoolwork. Don't let anything else on it distract you. Not for a minute, in any lesson, all day, every day.

Ask a student what their laptop is for, and very few will say "learning". It's their personal device. Schoolwork is one more thing it has to do.

That isn't a discipline problem. It's a design problem. Most adults would struggle with the same test.

Teachers absorb the shortfall

When the system can't help, the teacher becomes the system.

Without classroom-level visibility, a teacher's main tools are line of sight and asking students to close their laptops. That costs teaching time in every lesson. It also puts staff in the role of monitor rather than teacher, and that wears people down across a school year.

IT support: zero-touch or best endeavours

Unmanaged devices leave IT with two choices, and neither scales.

Some IT teams take a zero-touch stance. The device belongs to the family, so it's the family's responsibility. Keep it charged, keep it updated, keep it free of viruses. If it breaks, that isn't the school's problem.

That's a legitimate position. But is it still good enough? It made sense when the school network was the only way online, and the school already filtered it. It makes far less sense now that every student carries a hotspot, a VPN is a free download and AI can write a workaround in minutes. Stepping back from the device now means stepping back from the learning that happens on it.

Other IT teams take a best-endeavours approach and help where they can. But with no standard build, every fault starts from scratch, because every device is configured differently. IT can't push a fix, can't reimage a machine and often can't reproduce the problem. On paper, it's just a help desk. In practice, it carries a hidden technical overhead that grows every year.

Either way, the school is relying on a device policy it can't enforce. Minimum specifications, updates, antivirus, a charged battery: every one of them depends on families in very different circumstances keeping it up on their own.

> A device policy families have to enforce on their own isn't a policy. It's a hope.

Equity: protection shouldn't depend on home

Start with what every school says it wants: a good, fair experience for every student who walks through the gate.

On unmanaged devices, that experience varies from desk to desk. Not every app runs on every machine. The teacher plans one activity and ends up supporting five versions of it, while some students can't take part at all.

Then there's what happens at home. Some families set up parental controls, keep the device updated and talk about online safety over dinner. Others don't have the time, the confidence or the know-how. Each family's choices are reasonable on their own. Together, they mean a child's protection and learning depend on the home they come from.

So ask the question directly. Is the school's aim a fair, consistent experience for every student? If it is, an unmanaged programme can't deliver it, because the most important tool in the classroom has been left to chance. Managed devices give every student the same floor: the same tools, the same protection and the same chance to take part.

> *We wouldn't leave textbooks to chance. Why leave the device to it?*

After an incident, a clear record makes all the difference

Some of the hardest conversations in a school begin with a parent asking what happened.

When something serious happens, a school needs to know what was accessed, when, by whom, and how it was handled. On an unmanaged device, that picture is rarely complete.

The safety software may not be there. Schools often report that their safety software has stopped working. Usually it hasn't. It's been removed. Or the student was signed in with a personal account rather than their school one, so the activity sits under an identity the school doesn't control. Or the device was on a hotspot, and the school's logs show nothing at all.

A firewall log may show which device was involved, but not which student. Piecing together the rest takes time the school would rather spend supporting the student and their family. And it leaves the school explaining gaps in its record at the moment it most needs to be trusted.

A managed device closes those gaps, whoever owns it. The software stays on, the student signs in with their school identity, and the record shows who did what, and when.

> When safety software "stops working", it usually hasn't. It's been removed.



05

The rules keep changing

Most BYOD agreements were written for a world that has moved on many times since. In the last 12 months alone, three changes have landed. None of them changes who controls the device. All of them raise the stakes.

1. Phones are being banned. Their connection isn't.

- **Singapore:** from January 2026, secondary students can't use smartphones or smartwatches at any point in the school day, including recess.
- **South Korea:** a national law in force from 1 March 2026 bars students in primary, middle and high schools from using phones and smart devices in class.
- **Philippines:** DepEd Order No. 6, s. 2026 bans portable electronic devices during class time. In June 2026, the department told schools to enforce it strictly.
- **Vietnam:** Ho Chi Minh City extended its restrictions to recess from January 2026, after a pilot in 16 schools.
- **England:** KCSIE 2026, in force from 1 September 2026, says all schools should be "mobile phone-free environments by default".

Hong Kong and Thailand are debating similar moves. These bans are a good step. But a phone ban removes a device, not the internet that comes with it.

An unmanaged laptop can join the phone's hotspot and be off the school network in seconds. On a Mac linked to the student's phone, their messages arrive on the laptop screen, and iPhone Mirroring lets them use the phone itself from the laptop. On Windows, Phone Link brings texts, calls and notifications onto the PC. WhatsApp, games and social media all run on desktop too. The student doesn't need the phone in their hand.

On a managed laptop, the school's filter stays on whatever network the student joins, and the school decides which apps run. On an unmanaged one, the ban moves the phone out of sight and leaves everything else where it was.

> The phone goes in the bag. Its connection doesn't.

2. Expectations keep tightening, everywhere

Governments aren't only regulating phones. They're asking every part of a child's online world to do more, and to prove it.

- **Australia:** new industry codes took effect from December 2025 and March 2026. Pornography sites must now check users' ages, and as eSafety puts it, "clicking a button that says 'I am 18 years or older' is no longer good enough". Search engines blur explicit results by default, and app stores must stop under-18s downloading R18+ apps by September 2026.
- **Singapore:** from April 2026, app stores must screen users and stop those estimated to be under 18 from downloading inappropriate apps.
- **England:** KCSIE 2026 asks a named senior leader to review filtering and monitoring every year, and to check it works on every device in every relevant location. Through 2026, the Department for Education (DfE) has also updated its standards to cover generative AI. Section 6 looks at this in detail.

The pattern is the same everywhere. Platforms, app stores and search engines are being asked to check ages and filter content. Schools are being asked to supervise, monitor and keep a record.

Every one of those protections depends on knowing who is using the device. On a managed device signed in with a school account, they can work as intended. On an unmanaged one, a student can sign in with a parent's account or route around the checks with a VPN. The rules get tighter, but the gap an unmanaged device leaves stays the same size.

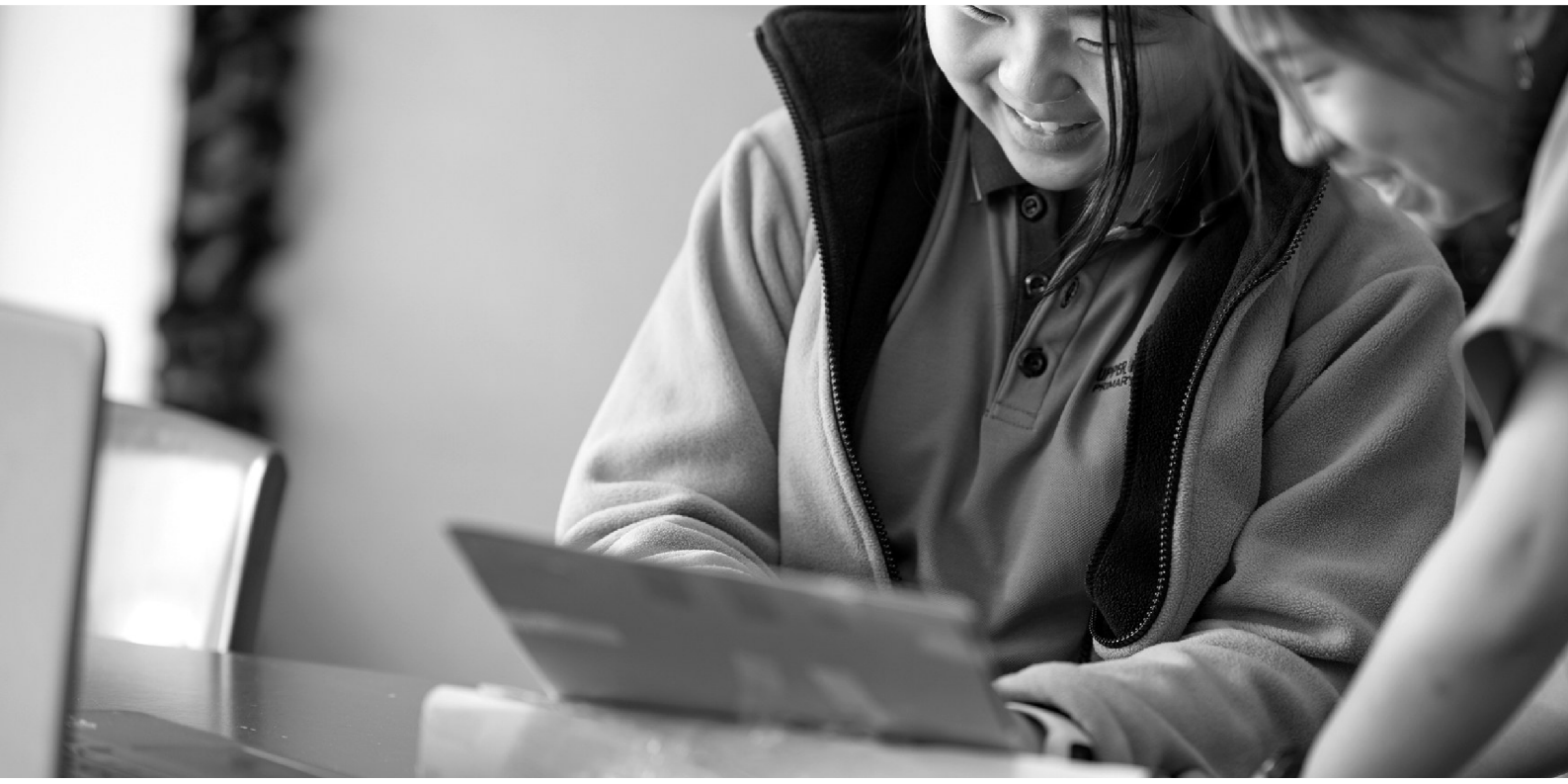
3. Age limits on social media spread. The behaviour stayed.

Australia's minimum age took effect in December 2025. Malaysia's Online Safety Act came into force in January 2026, Indonesia introduced under-16 restrictions in March 2026, and the UK announced its own in June 2026. The early evidence suggests the behaviour hasn't gone away. Three months in, the share of Australian under-16s using social media had only fallen from 85.9% to 81.5% (eSafety, July 2026).

The law didn't take the behaviour out of classrooms. It took away the assumption that someone else was handling it.

> Governments keep changing the rules. Nobody has changed the funding, and most schools haven't changed their device policy.

No regulation names a product. Each one names an outcome, and schools are increasingly asked to show how they meet it. On an unmanaged device, that can't be shown with any confidence.





06

KCSIE: a UK standard in a BYOD world

For British international schools, KCSIE is the benchmark. But it was written for a different device landscape.

British Schools Overseas aren't legally bound by Keeping Children Safe in Education (KCSIE). Their legal duties come from host-country law, and accredited schools also meet the BSO standards. But KCSIE is the reference point inspectors bring with them, many schools write it into their safeguarding policies, and it's the standard parents, governors and staff expect.

KCSIE was written for schools in England, where school-provided devices are the norm. School laptops are available in 94% of English secondary schools, and desktops in 98% (DfE, 2025). The DfE's filtering and monitoring standards are built around that. They define devices as "all internet connected devices managed by the school or college, even if they are taken home", and expect devices the school doesn't manage to sit on a separate network.

Apply that standard to a school where students bring unmanaged devices of their own, and the gap is built in. The standard assumes control the school doesn't have. A school with unmanaged BYOD isn't falling short of KCSIE through lack of effort. It's trying to meet a standard designed for managed devices without managed devices.

The people who feel it most

Many British international schools are led and staffed by people who trained and worked in the UK. They know KCSIE, they've been inspected against it, and they believe in it. Then they join a school where students hold the admin rights on their own devices, and find they can't do what they've always done, and what they believe is right.

That frustration is worth listening to. It's experienced safeguarding professionals telling the school that its device environment can't support the standard they hold themselves to.

What you must do, and what you choose to do

There's a difference between what a school is legally required to do and the standard it chooses to set for its students and its community. For many British international schools, KCSIE isn't the law. It's the standard they've chosen.

The device model decides how high that standard can go. On unmanaged BYOD, the ceiling is low: the school can filter its own network and little more. On managed BYOD, it rises: protections stay on and the record names the child. With school-provided devices, it's highest: every device identical and every control in place.

> The law sets the floor. Your device model sets the ceiling.

What the standards expect, and where an unmanaged device falls short

Expectation	What KCSIE and the DfE standards ask for	On an unmanaged device where the student is the administrator
Named responsibility	A member of the senior leadership team and a governor are responsible for meeting the standards. The designated safeguarding lead (DSL) acts on safeguarding concerns identified through monitoring and must understand the systems in place.	The senior leader is accountable for protections the student can switch off. The school is accountable. The student is in control. No review changes that.
Annual review	Review filtering and monitoring at least once every academic year. Check that filtering works on all internet-connected devices in all relevant locations, and keep a record.	The school can't test a device it doesn't manage. The review becomes a review of the network, not of the device the student actually uses.
Blocking bypass	Block technologies and techniques that get around the filter, such as VPNs, proxy services and end-to-end encryption methods. Filter all internet feeds, including backup connections and portable wifi devices.	A student administrator can install a VPN or proxy in minutes. A phone hotspot takes the device off the school's internet feed altogether.
Identifying the individual	Filtering logs should show the device name or ID, IP address and, where possible, the individual, with the time and date, so concerns can be traced back to a student.	Network logs see a device address, not a child. The DSL is left working out who was behind the screen.
Effective monitoring	Monitoring can combine in-person supervision, network monitoring and device monitoring using device management software.	Without device management, device monitoring isn't available. What remains is the network log and a teacher walking the room.
New technology, including generative AI	Reviews should be repeated when new technology is introduced, such as new devices or generative AI tools.	AI tools arrive on an unmanaged device whenever the student installs them, with no review at all.

Sources: Keeping Children Safe in Education 2026; DfE, Filtering and monitoring standards for schools and colleges (updated September 2026); SWGfL, July 2026.

The standards don't ignore BYOD. They say filtering should apply to unmanaged devices under a BYOD scheme, and that devices the school doesn't manage should sit on a separate network. That covers the device while it is on the school's network. It does nothing for the same device on a phone hotspot in the same classroom, or at home that evening.

Most of what KCSIE and the standards ask is written as "should", not "must". So the real question for a school isn't whether it complies. It's this: what is the best we can do in our environment, and is that good enough for the standard we've set ourselves?

How far can unmanaged BYOD go?

We mapped 18 expectations in KCSIE 2026 and the DfE filtering and monitoring standards against five device setups, and scored each as met, partly met or not met. The full scoring is in the appendix.

Device setup	All 18 expectations	14 technical expectations
Unmanaged BYOD, network filtering only	44%	36%
Plus a network-level monitoring tool	47%	39%
Plus parental controls set up by families, and structured staff training	58%	46%
Managed BYOD (school holds admin)	97%	96%
Managed school-provided devices	100%	100%

At best, about 60%.

Even with network monitoring, parental controls and structured staff training, an unmanaged BYOD programme reaches about 60% of KCSIE's filtering and monitoring expectations, and less than half of the technical ones. The other 40% depends on controlling the device.

Linewize analysis of KCSIE 2026 and the DfE filtering and monitoring standards. Scores show whether an expectation can be met in each setup. They are not a guarantee of safety.

Where the gap shows

The gap rarely shows on an ordinary day. It shows at three moments, and each one lands on a named person.

The annual review

KCSIE asks the senior leader responsible for filtering and monitoring to check, at least once a year, that filtering works on all internet-connected devices in all relevant locations, and to keep a record. For school-managed devices, IT can test this and write it down. For an unmanaged laptop, the honest record reads something like: filtering works while the student is on our network and chooses not to bypass it. Few senior leaders would want to sign that.

The incident

A monitoring alert or a parent's concern reaches the designated safeguarding lead. The log shows a device address and a time. It doesn't show a name, and anything that happened over mobile data or a VPN isn't there at all. KCSIE expects the DSL to understand the school's filtering and monitoring well enough to act. On an unmanaged device, they are acting on half the picture.

The inspection

An inspector asks how the school knows its safeguards work on students' own devices. "We ask students not to switch them off" is an honest answer. It isn't a reassuring one.

> KCSIE puts the accountability with the school's senior leaders. On an unmanaged device, the controls sit with the student.

Boarding schools face the sharpest version

For boarding schools, the BSO standards are already explicit. The child protection policy should cover how boarders' devices are managed when they bring them into school, and "the opportunity to download harmful content via 3, 4 and 5G that will bypass the school's filtering and monitoring systems". Schools are also expected to run proportionate systems to monitor and control electronic communications.

Evenings and weekends are when boarders are online most and supervised least. A network filter can't reach a device on mobile data in a boarding house. Only protection on the device can.

Source: Department for Education, Standards for British Schools Overseas, boarding standards 8.4 and 12.1.

What closes the gap

None of this means a British international school has to replace every family's laptop. It means making three decisions that KCSIE already implies.

- **The school holds administrative control of every device used for learning, whoever owns it.** The person the safeguards protect can't switch them off.
- **Filtering and monitoring live on the device.** Protection that travels with the student works on the school network, on a hotspot and at home. That is what "all relevant locations" asks for.
- **The record names the child.** Device-level software ties activity to a signed-in student, with the time and date, so the DSL can act and the senior leader can evidence the review.

Close those three gaps, and the 60% ceiling is gone. The annual review becomes a record the school can stand behind, not a description of its network.



07

Privacy, trust and parent choice

Managed BYOD only works when families trust it. Be clear about what the school can see, when and why. Then give parents real choices.

Singapore offers a useful model. Secondary students' Personal Learning Devices come with a Device Management Application. By default, the Ministry of Education and the school set the web filtering level, and a parent account lets parents see their child's device activity. After school, parents can keep the school's settings, change them or switch them off (Damai Secondary School, MOE). The school still manages the device. Parents adjust a safety layer on top, without admin rights.

Strong protection during school hours, with family choice at home, is far easier for parents to accept than full school control. The aim is not to extend the school into every part of family life. It is to remove the confusion about who is protecting the child, and when.

- Explain what you can see, and what you can't, in plain language and in the languages families use at home.
- Set clear hours, and say which rules apply in school and after school.
- Collect only what you need, and say who can see student data and how long you keep it.
- Check local privacy law. Data protection laws differ across the region, so ask your legal adviser what applies to you.

What families get in return

Asking families to hand administrative control to the school can sound like taking something away. Done well, it's the opposite.

The school takes responsibility for the device while it's used for learning. In return, parents get something most have never had: clear visibility of what happens on their child's device, and simple controls for after school hours. Built-in parent controls let families see activity, pause the internet and set limits at home, on the same device the school manages during the day.

That changes the conversation. It isn't "hand over your child's laptop". It's "let us manage it for learning, and we'll give you tools you don't have today".

Most parents want what the school wants. When full management is a condition of using a device for learning, and it's explained clearly, very few families object. Most see a school taking a stance that matches their own values as parents.

> It isn't about taking control away from families. It's about giving them something back.



08

The best you can do. Is it enough?

Most schools running BYOD are already doing the best they can with the devices they have. The harder question is whether that's good enough for the standard they've set themselves.

Moving from unmanaged to managed rests on four foundations:

01

Students are standard users, not administrators.

This is the control that holds up everything else.

02

Every device used for learning is enrolled in device management.

It's a condition of use, written into the BYOD agreement and renewed every year.

03

Parents are on board.

They understand the programme, can see what it gives them, and support it at home.

04

Filtering lives on the device.

Protection travels with the student, on any network, at any hour.

Get the four foundations right, and the rest follows: classroom tools teachers can use in real time, after-hours visibility for families, and one clear record for wellbeing staff. They're the result of managing the device, not the starting point.

Some honest questions for your next leadership meeting

Managing devices isn't about one benefit. It's about the security of your devices and network, the safety of students online, and protecting the learning in your classrooms. So the questions cover all three.

In the classroom

Do your teachers raise concerns about what students are doing on their devices during lessons?	Yes / No
Is digital distraction (games, social media, messaging) a problem in your classrooms?	Yes / No

Student safety

Do students use VPNs, proxies or hotspots to get around your filter?	Yes / No
If a student were having an inappropriate conversation with another student on their laptop right now, would you know?	Yes / No
If a parent asked what happened on Tuesday, could you tell them, in language they'd understand?	Yes / No

Devices and network

Do students hold administrator rights on the devices they learn on?	Yes / No
Could you say, with confidence, which devices on your network are being used for learning, and who controls them?	Yes / No

Now look back at your answers. Are you comfortable with them? Are you happy for things to stay as they are?

If you are, that's a fair position.

If you're not, that's the uncomfortable truth this paper is about. Where you are today isn't good enough for the standard you've set for your school. And that's the point to start changing it.

Which of these answers are you comfortable with?

09

You may already have most of what you need

This may be a policy decision, not a purchase.

When schools think about managing devices, many start with the budget: new hardware, new software, a project with its own line item. That's usually the wrong place to start. Much of what's needed is already included in licences the school pays for today. What's missing is the decision to use it.

The real first step is setting the direction. Every device used for learning will be managed, and students won't be administrators. Write that into policy and the BYOD agreement. The technology question comes after, and it's usually smaller than expected.

> Start with the decision, not the budget.

Before pricing anything new, find out what you already have. These three questions, put to your IT team, will usually give you the answer.

1. **"Are we using the device management that comes with our Microsoft licence?"** Most schools on Microsoft 365 Education have device management included. Some use it fully. Others use only a small part of it.
2. **"Did our Chromebooks come with the management upgrade?"** Chromebooks bought through an education supplier often include it in the price. If yours did, the school may already have the tools to manage them properly.
3. **"Are any of our school-owned Macs or iPads outside device management?"** Apple's school enrolment service is free. If some school-owned Apple devices aren't enrolled, this is often the simplest and lowest-cost gap to close, usually within a term.

In a school group, these decisions may have been made centrally, so your group IT team may be the right people to ask. Licence names and bundles also vary by country and supplier, so confirm details with your local education partner. A licensing summary for IT teams is in the appendix.

A laptop is a laptop

It doesn't matter who paid for it. A device used for learning is a device used for learning. If the school has the tools to manage it and the will to manage it, it can manage it, whoever's name is on the receipt.

The real question is how the school wants that device treated, and whether everyone with a stake in the child's use of it agrees. That means the school, the family and the student sharing the same vision, the same story and the same message.

If the answer is yes, the device can be managed. That's why the BYOD agreement matters more than any tool. The technology is largely paid for already. What schools need is families' agreement on how it's used.

A laptop is a laptop. It doesn't matter who paid for it.

The sentences that matter in a BYOD agreement

Most of the distance between unmanaged and managed is covered by a few sentences in the BYOD agreement. Very few families object to them, provided they're offered as a partnership: the school takes responsibility for the device, and families get something back.

> *"Every device used for learning at this school, whoever owns it, is fully managed by the school while it is used for learning, and released to the family when it leaves the programme."*

> *"Students use a standard account on their learning device. The school holds administrator access, so the protections on the device stay in place."*

> *"The school's safety software runs whenever the device is used for learning, in school and at home. In return, parents have their own visibility and controls for after school hours."*

> *"Learning devices must meet the school's specification, including the chosen platform."*

Have your legal adviser check the wording for your country and school type.

Device management is the foundation, not the whole answer. Schools still need filtering that travels with the student, classroom tools for teachers and support for families, from whichever provider they choose. And no single tool protects students from every online risk. Technology works best alongside digital literacy education, trusted adults, clear policy and staff who feel confident using it.

10

Where to start

This paper doesn't say every school has to change. It asks whether where you are today is good enough for the standard you want to set. If it is, that's a fair position. If it isn't, here's how to start.

Start with what you want to achieve. That might be meeting as much of KCSIE as you can. It might be keeping games out of lessons. It might be knowing, at any time, if a student may be at risk of harm. Whatever it is, the next question is how much change your school is ready for.

1

Agree your standard

Discuss it as a leadership team and agree what your standard looks like: for safety, for learning and for your community. Then agree that this is what the school will stand for. Define the standard before you think about how to enforce it.

2

Check you have the ability

Can you make it happen? Talk to your IT team about the device management you already pay for, and about what support you'd need from outside. Many schools find more is in place than they expected.

3

Check you have the appetite

Moving to managed devices takes leadership commitment, not just IT effort. Some families and some staff will push back. That's normal, and it's part of the journey. Decide now that you'll see it through.

4

Bring parents with you

Don't dictate. Ask. Share the vision before the detail. If parents hear "we're doing this for control", they'll push back. If they hear "we're doing this for the best outcomes for your children", most will follow. Talk about what managed devices make possible, not what students might do wrong. And be clear about what families get in return.

5

Build a plan

You'll need three things in place: IT support, leadership support and parent support. Explore the funding options in your region, including leasing and parent-funded device schemes. Then decide your pace. Many schools phase it in over three years, starting with entry year groups such as Year 7 and Year 10 and adding year groups each year.

6

Decide whether the pace matches the risk

A three-year plan means three more years of today's problems for some students: the distraction in class, the risks online and the gaps against the standard you've set. Is that acceptable? If not, move faster where it matters most.



If your school runs unmanaged BYOD, the *best* you can achieve is about 60% of KCSIE's filtering and monitoring expectations.

Linewize analysis of KCSIE 2026 and the DfE filtering and monitoring standards. See section 6 and the appendix.

A

Appendix: for IT teams

Platform quick reference

Platform	Management options	What to review
Microsoft Windows	Microsoft Intune and Intune for Education	Existing licences, device enrolment, app deployment, configuration policies and administrator rights
Google ChromeOS	Google Admin console and ChromeOS device management	Device enrolment, Chrome Education Upgrade licences, browser policies and app restrictions
Apple macOS and iPadOS	Apple School Manager with a device management platform	Automated enrolment, supervision where supported, configuration profiles, app deployment and limits on personally owned devices

Management capabilities depend on operating system, device ownership, enrolment method and licensing. Verify current platform requirements before making changes.

Bringing a family-owned device under management

Taking full control of a family-owned laptop usually means enrolling it from a reset, the way a school device would be set up. Tell families this before they agree, and set out in the BYOD agreement how the device is released when the student leaves the programme.

IT readiness checklist

- We know which student devices are managed and which are not.
- We know which students have administrator rights.
- We can verify that the required safety software is installed and running.
- We have tested protections on and off the school network.
- We know which browsers, apps and networks our safeguards support.
- We have reviewed our existing management licences and what they include.
- We know what information the school can access and how privacy is protected.
- We have a clear process for devices that don't meet school requirements.
- Our BYOD agreement explains the responsibilities of the school and of families.

KCSIE scoring: how we reached the numbers

Each expectation is scored Met (1), Partly met (0.5) or Not met (0) for each setup. The first four expectations cover roles and the annual review. The other fourteen are technical. "Parental controls" means consumer controls set up by families, family by family: they help at home, but they aren't consistent across a school and their data goes to the parent, not the school.

Expectation	Unmanaged, network only	+ network monitoring	+ parental controls and staff training	Managed BYOD	School-provided
Roles: named SLT member and governor responsible	Met	Met	Met	Met	Met
Roles: DSL leads on concerns and understands the systems	Partly	Partly	Met	Met	Met
Roles: staff trained on expectations, roles and escalation	Partly	Partly	Met	Met	Met
Review: at least annually, led by SLT, and recorded	Met	Met	Met	Met	Met
Review: checks filtering works on all devices in all relevant locations	Not met	Not met	Not met	Met	Met
Review: assurance that solutions keep working on all devices after changes	Not met	Not met	Not met	Partly	Met
Filtering: blocks illegal content and can't be switched off	Partly	Partly	Partly	Met	Met
Filtering: blocks bypass (VPNs, proxies, encryption methods)	Partly	Partly	Partly	Met	Met
Filtering: covers all internet feeds, including backup connections and portable wifi	Not met	Not met	Partly	Met	Met
Filtering: protection continues off site and at home	Not met	Not met	Partly	Met	Met
Filtering: logs show device, IP, individual, time and date	Partly	Partly	Partly	Met	Met
Filtering: concerns can be traced back to an individual	Partly	Partly	Partly	Met	Met
Filtering: blocks harmful content without unreasonably affecting teaching	Met	Met	Met	Met	Met
Filtering: filtering and monitoring applied to generative AI use	Partly	Partly	Partly	Met	Met
Monitoring: combines in-person, network and device monitoring	Partly	Partly	Partly	Met	Met

Expectation	Unmanaged, network only	+ network monitoring	+ parental controls and staff training	Managed BYOD	School-provided
Monitoring: device monitoring using device management software	Not met	Not met	Not met	Met	Met
Monitoring: concerns surface quickly to the DSL for action	Not met	Partly	Partly	Met	Met
Monitoring: unmanaged devices kept on a separate network	Met	Met	Met	Met	Met

Linewize analysis of Keeping Children Safe in Education 2026 and the DfE Filtering and monitoring standards for schools and colleges (updated September 2026). Scores show whether an expectation can be met in each setup, not a guarantee of safety.

Glossary

- **BYOD:** Bring Your Own Device. Students use a device their family owns for school learning. BYOD is one form of 1:1.
- **1:1 programme:** Every student has their own device for learning. The device may be owned by the family (BYOD) or by the school.
- **Managed device:** A device the school manages as if it owned it, with administrative control held by the school. Being enrolled in device management is not enough on its own.
- **Admin rights:** The highest level of access on a device. A person with admin rights can install or remove any software.
- **Standard user:** An account that can use the device but can't change important settings or remove protected software.
- **Device management (MDM):** Software that lets a school set up, update and protect many devices from one place.
- **Safety software:** Software on the device that filters content and helps the school and parents see activity.
- **VPN:** A tool that hides internet activity. Students sometimes use one to get around school filtering.
- **Proxy:** A website or tool that loads blocked pages through another server, so the filter can't see them.
- **Hotspot:** A phone sharing its mobile data connection with another device, taking that device off the school network.
- **KCSIE:** Keeping Children Safe in Education, the Department for Education's statutory safeguarding guidance for schools in England.

Sources

- BeyondTrust, Microsoft Vulnerabilities Report, 13th edition, 2026 (section 3)
- Center for Internet Security, CIS Critical Security Controls v8.1 (section 3)
- DQ Institute, Child Online Safety Index 2023 (section 4)
- Microsoft Global Online Safety Survey 2025 (section 4)

- UNICEF, ECPAT and INTERPOL, Disrupting Harm in the Philippines, 2022 (section 4)
- Linewize, How your students are getting around the web filter, May 2026 (section 4)
- Childnet, Young people's use of VPNs, December 2025 (section 4)
- Steinberg et al., Around the world, adolescence is a time of heightened sensation seeking and immature self-regulation, Developmental Science, 2018 (section 4)
- Steinberg et al., Age differences in future orientation and delay discounting, Child Development, 2009 (section 4)
- Ministry of Education Singapore, announcement on smartphone use in secondary schools, November 2025 (section 5)
- Republic of Korea, Elementary and Secondary Education Act revision, August 2025 (section 5)
- Department of Education Philippines, DepEd Order No. 6, s. 2026 and memorandum of June 2026 (section 5)
- Ho Chi Minh City Department of Education and Training, September 2025 (section 5)
- eSafety Commissioner, industry codes and age assurance FAQs, 2025 to 2026 (section 5)
- Infocomm Media Development Authority, Code of Practice for Online Safety for App Distribution Services, 2025 (section 5)
- Mayer Brown, Malaysia's Online Safety Act in focus, July 2026 (section 5)
- eSafety Commissioner, social media minimum age evaluation, 31 July 2026 (section 5)
- Department for Education, Keeping Children Safe in Education 2026 (sections 5 and 6)
- Department for Education, Filtering and monitoring standards for schools and colleges, updated September 2026 (section 6)
- Department for Education, Technology in schools survey 2024 to 2025 (section 6)
- Department for Education, Standards for British Schools Overseas (section 6)
- ISI, BSO Inspection Handbook, September 2025 (section 6)
- SWGfL, KCSIE 2026: what schools need to know, July 2026 (section 6)
- Damai Secondary School (MOE Singapore), Device Management Application (section 7)

BYOD isn't the problem. Losing control of the device is.

Every school that runs BYOD well made the same decision: management. The school decides what the device can do, not the student.

The question for yours is whether, and when, you make it too.

Linewize
by Qoria

Want to talk it through?

If this paper raised questions for your school, we're happy to talk them through, wherever you're starting from.

enquiries@linewize.io

Linewize
by Qoria

Linewize creates school communities that free our kids to get the best out of the digital world, while protecting them from harm.

Web: www.linewize.io
Email: enquiries@linewize.io

Linewize is part of Qoria, a global technology company dedicated to keeping children safe and well in their digital lives. We harness the power of connection to close the gaps that children fall through, and to support them on all sides - at school, at home and everywhere in between.

Find out more **www.qoria.com**