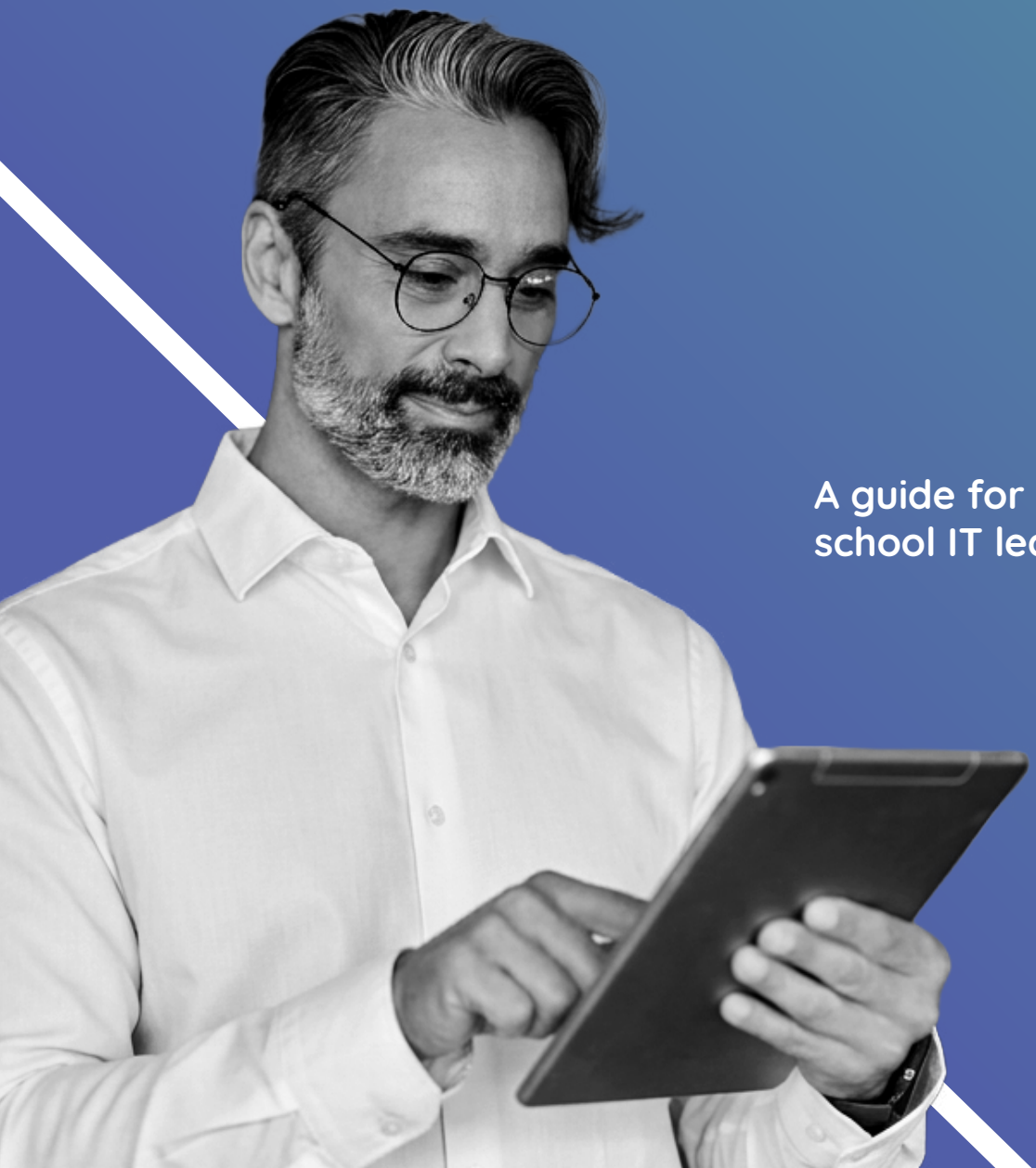
Qoria

How managed devices help you meet UAE child digital safety rules



A guide for UAE school IT leaders

qoria.eu

Contents

01 The problem with unmanaged devices **03**

02 Admin rights: the decision behind every other control **04**

03 What the UAE rules expect **05**

04 Protection beyond the school gate **06**

05 What good looks like **07**

06 You probably already own the tools **08**

07 How Qoria helps **09**

The problem with unmanaged devices

“Students keep getting around the filter, and BYOD makes it worse.”

We hear this from IT managers across the UAE. Bring Your Own Device got technology into every classroom fast, and for many schools it still works. But learning moved onto those devices, and the school’s ability to see and shape what happens on them didn’t keep up.

Schools often debate BYOD versus 1:1. The bigger difference is whether a device is managed or unmanaged.

	Unmanaged BYOD	Managed BYOD	Managed 1:1
Who owns the device	The family	The family	The school
Who administers it	The student	The school, by agreement	The school
Filtering	Network only. Stops at the school gate	On the device. Goes where the student goes	On the device. Always on
Classroom control	Ask, and hope	Teacher-led, in real time	Teacher-led, in real time
IT support	Every device is a special case	Standard setup, fixed remotely	One fleet, one process
Evidence after an incident	Whatever the firewall logged	A record for each student	A record for each student

Between the first two columns, families still own the device. What changes is who administers it. For most schools, moving from unmanaged to managed BYOD uses devices and licences they already have, although some older devices may not support management.

Admin rights: the decision behind every other control

On an unmanaged BYOD device, the student is the administrator by default. Nobody decided it; it's how the device comes set up.

That means a student can:

- Uninstall the 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
- Change DNS settings, turn off updates and disable antivirus
- Install anything, from anywhere

Your digital policy, your filter and your wellbeing programme all assume those protections are still running in fifth period. If a student can remove them, they only work when the student chooses to leave them on.

Student behaviour isn't the issue here; device settings are. Give a year group devices where the safety software can be switched off, and within a term one student will work out how. By the end of that week, most of the year group will know.

40% of all vulnerabilities Microsoft disclosed in 2025 were elevation of privilege: attacks that turn a standard user into an administrator. On an unmanaged student device, the student already has those rights.

Source: BeyondTrust, Microsoft Vulnerabilities Report, 13th edition (2026)

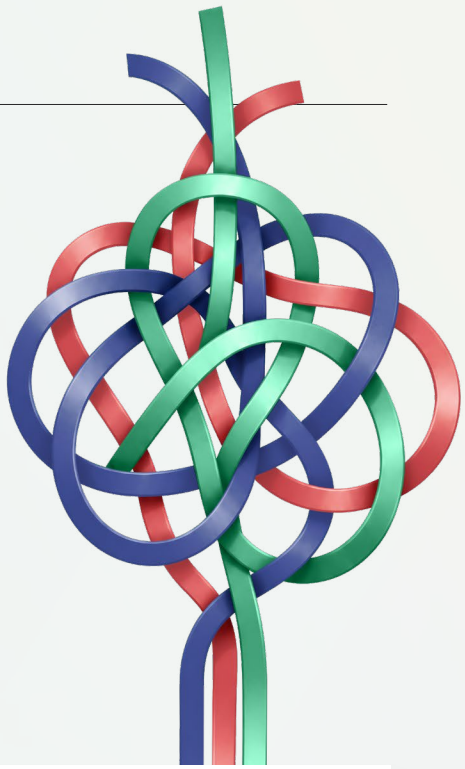
The fair objection

You can't strip admin rights from a laptop a family paid for. That's a fair point, and it's why most BYOD programmes stay unmanaged.

The middle path is to make managed enrolment a condition of using a personal device for learning. Write it into your BYOD policy, explain it to parents in plain language, and renew it every year. Most families agree once they see it as protection for their child.

In Abu Dhabi you already need this policy: **ADEK requires schools to set rules for personal devices and define safety precautions for BYOD**. In a school group, the decision usually sits with group IT and leadership, so raise it there.





What the UAE rules expect

UAE schools answer to up to three frameworks. Each one asks for an outcome, and each outcome depends on protections staying in place on the device.

Federal Child Digital Safety Law.

In force since 1 Jan 2026, with a general deadline to comply by 1 Jan 2027 unless the Cabinet extends it. Applies to every family in the UAE.

ADEK School Digital Policy.

In effect now for Abu Dhabi private and charter schools.

KHDA Inspections.

Returning in 2026-27 for Dubai private schools, at no more than 24 hours' notice, with student wellbeing in focus.

The rule asks	On an unmanaged device
Filter and monitor student internet use on school devices and systems (ADEK §4.2.2(b))	The student can remove the agent
Restrict student VPNs on school premises and networks (ADEK §4.1.2(a))	An admin user installs one in a minute
Set rules and safety precautions for personal devices (ADEK §4.1, §5.1)	A rule the student can override is only a request
Spot worrying trends and filter violations (ADEK §4.2.2(c))	No signal from devices you can't see
Record every digital incident for audit (ADEK §4.3.3)	Firewall logs show a device, not a child
Show inspectors how you look after student wellbeing (KHDA 2026-27 inspections)	No evidence to show at 24 hours' notice

UAE rules describe outcomes and don't name products. ADEK requires filtering on school devices and systems, and asks schools to set safety precautions for BYOD. Showing that students stay safe on a device the school doesn't manage is hard, which is why many schools choose managed devices.

Sources: Decree-Law 26/2025, Art. 18 · ADEK Digital Policy v1.1 · KHDA announcements, May 2025 and 2026

Protection beyond the school gate

Network filtering stops at the school gate.
UAE rules reach into the home.



Network filtering protects the network, but students stopped depending on it years ago. A phone hotspot, a free VPN or a portable browser on a USB stick takes a student outside your filter without leaving the classroom. On a managed device, each one is blocked at the source. On an unmanaged one, it takes two minutes, and the method spreads through a year group in days.

Then the device goes home, and UAE rules follow it there:

- Federal law asks parents to monitor their children's online activity and use parental controls (Decree-Law 26/2025, Art. 13(a)).
- In Abu Dhabi, ADEK requires schools to require parents to monitor device use outside school (ADEK §4.4).

On an unmanaged device, a child's safety depends on what their family can set up at home. A managed device gives every student the same protection on any network, at any hour, and lets parents see the same activity the school does.

46% of compromised systems holding company logins were non-managed devices, carrying both personal and work credentials outside any management programme.

Source: Verizon 2025 Data Breach Investigations Report

Protection that lives on the device makes managed BYOD possible, whoever owns the laptop.

What good looks like

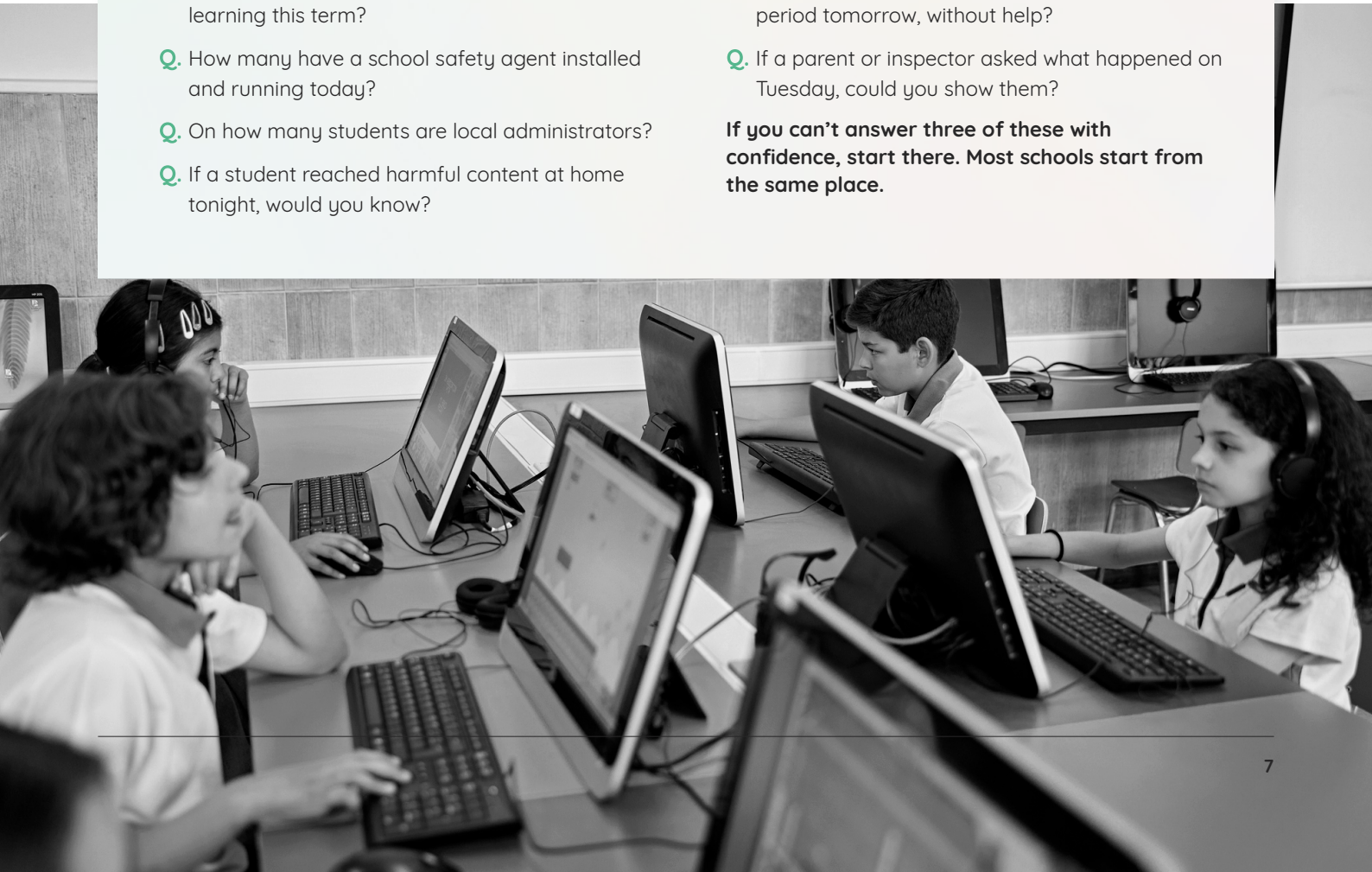
Managed BYOD means seven things are in place at the same time. Most schools already have two or three of them.

1. **Enrolment is a condition of use.** Every device used for learning is enrolled, personal ones included. It's in the BYOD policy and renewed each year.
2. **Students are standard users.** This is what keeps the other six in place.
3. **Filtering lives on the device.** Protection goes with the student, on any network, at any hour.
4. **The safety agent resists tampering.** Students can't switch it off or uninstall it.
5. **Teachers have real-time classroom tools.** They can guide screens during the lesson, without raising a ticket.
6. **Families can monitor online activity** after school hours and can set limits at home.
7. **There's one record.** It's consistent for each student, and wellbeing staff can read it as easily as IT can.

Checklist for the IT team at the school

- Q. How many personal devices are used for learning this term?
- Q. How many have a school safety agent installed and running today?
- Q. On how many students are local administrators?
- Q. If a student reached harmful content at home tonight, would you know?
- Q. Could a teacher guide student screens in the third period tomorrow, without help?
- Q. If a parent or inspector asked what happened on Tuesday, could you show them?

If you can't answer three of these with confidence, start there. Most schools start from the same place.



You probably already own the tools

Managing devices sounds like a new budget line. For most schools it's a licence they already pay for and a console nobody has opened.

Check before you price anything. In a school group, group IT usually holds these licences.

Platform	What you may already have	Watch out for
Windows (Microsoft 365 Education)	Intune for Education is included in A1 and manages Windows and iPad. Windows LAPS and AppLocker are built in at no extra cost	Full Intune Plan 1 needs A3 or A5. Endpoint Privilege Management, which lets students run as standard users, is a paid add-on
ChromeOS (Google Workspace for Education)	Education Chromebooks often ship with the ChromeOS Education Upgrade included. Chrome Browser Cloud Management works on family-owned PCs and Macs	The free Education Fundamentals tier alone does little for device policy
Apple (school-owned Macs and iPads)	Apple School Manager is free and, with an MDM, makes devices supervised: students can't remove the management profile	Jamf is quote-priced. Mosyle has a free tier, with paid tiers for privilege management

Check this week: which Microsoft tier you're licensed for, whether your Chromebooks came with the upgrade, and whether any school-owned Mac or iPad sits outside an MDM. That last one is usually the cheapest gap to close.

What the tools can't do

On a family-owned Windows PC or Mac, no vendor can remove the owner's admin rights without their agreement. That's why your BYOD policy matters as much as the technology. Most of the tools are already paid for, and the policy gives you permission to use them.

Three clauses for your BYOD policy

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

1. Devices used for learning are enrolled in the school's management system for as long as the student is enrolled.
2. Students use a standard account on their learning device. The school holds administrator access.
3. The school's safety software runs whenever the device is used for learning, at school and at home, and parents can see the same activity the school can.

How Qoria helps

Device management keeps devices secure. Qoria keeps students safe.

Intune, Google Admin and Jamf give you a secure, well-run device. They don't protect a 14-year-old online at 9pm, help teachers keep a lesson on track, or support parents at home. Qoria works alongside whatever manages your devices, protecting students in class, at home and everywhere in between.

	Protect every device	See and respond	Extend to home
What it does	Filtering that goes with the device, VPN and proxy blocking, teachers guiding screens in class	Early-warning alerts, an evidence trail for every incident, wellbeing insights	A parent app families use, with one setup for school and home
Qoria solutions	Qoria Filter · Classroom Manager	Qoria Monitor · Pulse	Qustodio
Rules it supports	ADEK §4.2.2(b), §4.1.2(a), §4.1	ADEK §4.2.2(c), §4.3.3 · KHDA inspections	Decree-Law 26/2025, Art. 13(a) · ADEK §4.4

> **"From my experience of KHDA and ADEK inspections, they want evidence of what we're doing for wellbeing, but it doesn't stop there.** They also want to see the impact: what changes you're seeing in students over time, and the feedback you're getting from students, parents and staff."
>
> **Emily Joy Partridge, Lead School Counselor · Kent College Dubai**

Where to start

1. **Count your devices.** Count the devices used for learning, the safety agents installed and running, and the students with admin rights.
2. **Open the consoles you already pay for.** Check your Microsoft tier, your Chromebook upgrades, and any Apple devices outside an MDM.
3. **Make the admin-rights decision at leadership level.** It's a duty-of-care question, so write it into your BYOD policy before an incident happens.
4. **Choose protection that lives on the device.** It works the same way whether the family or the school owns the laptop.

Sources: Federal Decree-Law 26/2025 · ADEK School Digital Policy · KHDA: inspections resume in 2026-27 · KHDA Wellbeing Matters.
Plain-language summary for information only, not legal advice. Always check the official texts. Sources last checked 9 Oct 2026.

Qoria

Not sure where your school stands?

Book a 30-minute review with our UAE team. We'll look at the rules that apply to you and what to prioritise first.

Contact us: **enquiries@qoria.eu**

qoria.eu