Smartphones, Safeguarding and the School's Digital Duty of Care

Moving Beyond the Choice Between Banning Phones and Monitoring Everything

A Thought-Leadership Discussion Paper for School Leaders

LATEST DISCUSSION EDITION | OCTOBER 2026

Authors

Dr Vincent Watters

Advocate Nicholas J Tee

Edition and review caveat

This is a working opinion piece prepared for discussion and professional review in October 2026. It may be refined following feedback from school leaders, ISASA and legal or safeguarding reviewers. Readers should check the WE&ESS Resources page for the latest edition.

This article expresses a viewpoint for discussion. It is not legal advice, a statement of settled law, nor a universal policy prescription. Schools should obtain advice appropriate to their own circumstances when developing or reviewing policies.

Correspondence: info@we-ess.co.za

Prologue — A Thought-Leadership Discussion

This article is deliberately presented as a thought-leadership discussion rather than as a prescription for how every school should manage mobile phones and digital devices.

Schools operate in very different environments. What is appropriate for one school may not be appropriate for another. A boarding school, a day school, a rural school, an urban school, a primary school and a senior secondary school may all have different risks, resources and expectations from their parents and governing bodies.

We may have to agree to disagree — without being disagreeable.

The purpose of this discussion is not to tell schools whether they should ban phones, permit them, restrict them or use technology to manage access. It is to ask a more fundamental question:

Does every school know exactly what its policy is, where it applies, what it is intended to protect learners from, and what responsibilities that policy creates for the school, the learner, the parent and the educator?

That question becomes increasingly important as the boundaries between the physical school and the digital world become less clear.

What Do We Mean by "School"?

For the purposes of this discussion, we use the word ***school*** more broadly than simply the physical school campus.

A learner may be under the supervision and care of a teacher on a sports tour, school trip, camp, excursion, cultural activity, school function or school transport. The physical location may have changed, but the school's responsibilities and duty of care have not necessarily disappeared.

This matters particularly when we consider mobile phones. A phone on a school campus is one thing. A phone in the hands of a learner on a school bus, at a sports tournament, on a hike, in a hotel during a school tour or in a boarding environment can create very different circumstances — and therefore may require different rules. We contend that:

The policy needs to follow the circumstance, not simply the building.

Smartphones Are Now Part of School Life

Smartphones are now an established part of everyday life for most young people. They provide obvious benefits for communication, learning, navigation and access to information. They also create risks that schools cannot simply ignore: cyberbullying, harmful or age-inappropriate content, online harassment, inappropriate recording and sharing, peer pressure, grooming and exposure to material that a learner may never have encountered without a connected device.

For school leaders, the question is therefore no longer whether smartphones present a safeguarding challenge.

The more difficult question is how schools should manage that challenge in a way that is effective, proportionate and practical — without turning teachers into full-time phone police.

This is becoming particularly important because the traditional debate has often been presented as a choice between two approaches:

Ban the phones.

Or:

Monitor the phones and, as in some cases, monitor down to keystrokes on a Learner's phone.

But perhaps there is a third option.

The Real Safeguarding Question Is Bigger Than "What Sites Are Learners Visiting?"

The digital safeguarding discussion is sometimes framed as though the principal risk is that a learner will deliberately search for something inappropriate. That certainly happens. But it is only part of the problem.

The risk can also be what comes looking for the learner.

A learner does not necessarily have to search for pornography, gambling or other inappropriate material to encounter it. A simple search for a football team, a sporting result or another popular interest can generate advertising, recommendations, links or invitations from services that the learner neither expected nor understood.

Similarly, grooming does not necessarily begin with a learner deliberately looking for a grooming site. Gambling does not necessarily begin with a learner deciding to visit a gambling website. Identity theft, phishing, scams and manipulation can begin with apparently innocent interactions.

Games and social platforms can create their own environments for communication and contact. Platforms such as Roblox, for example, can provide social and communication environments as well as gameplay. The safeguarding question therefore has to include not only what a learner deliberately seeks out, but what digital services can expose the learner to, who can contact the learner, what content can be shared, and what information can be harvested.

The issue is therefore not confined to learners trolling the internet for undesirable material. It includes risks and behaviours directed at learners — including grooming, cyberbullying, exploitation, scams, gambling, identity theft and inappropriate contact.

This changes the question. It is not simply:

"Can we stop learners visiting undesirable websites?"

It is more likely to be:

"What digital environment is appropriate for our learners, in this particular circumstance, and how do we provide it?"

What are schools actually doing?

Schools are taking a variety of approaches.

Some have introduced complete or near-complete phone bans during the school day. Others require phones to be handed in, stored securely or placed into individual lockable pouches. Some allow phones but establish detailed Acceptable Use Policies (AUPs), defining when and how they may be used.

Others rely heavily on the school's Wi-Fi filtering and monitoring systems, while an increasing number are considering more sophisticated digital safeguarding technologies.

Each approach has merit. None completely solves the problem.

A phone ban can be effective in removing distraction from the classroom. Physical collection or storage can go further by removing the device from immediate use.

Lockable magnetic pouches have become another practical solution. They allow learners to retain possession of their phones while restricting normal access during the school day.

It still requires the school to ensure that the correct device is in the pouch, that the pouch has been properly secured and that learners are not tampering with the system. It also leaves schools with the continuing problem of what happens when the normal school day ends.

Most importantly, a phone ban does not make the digital world disappear.

A learner may have another device. They may have access to mobile data. They may find ways around a physical restriction. Or they may simply wait until the opportunity presents itself.

The issue, therefore, is not whether a school can create a rule.

It is whether the school can manage the digital environment in which learners operate.

The Department of Basic Education's Guidelines on e-Safety in Schools provide an important point of reference. They caution against treating an outright ban as a complete answer and emphasise managing mobile-device use through clear acceptable-use expectations.

"Outright banning of the use of mobile devices in a school can be self-defeating and educationally unsound."

The guidelines go on to say that schools have a responsibility to manage the mobile-device environment and that an Acceptable Use Policy should specify "when and for what purpose" mobile devices may be used, with steps to ensure compliance.

This is significant.

The DBE is not suggesting that schools simply allow unrestricted smartphone use. Rather, it recognises that the modern school needs to manage mobile-device use according to context and purpose.

That creates a much more interesting question for school leaders. Instead of asking:

"How do we stop learners using their phones?", perhaps the question should be:

"How do we ensure that learners use their phones appropriately while they are under our supervision?"

That is a fundamentally different proposition.

The problem is not the majority, as most learners will follow a reasonable school policy.

They will put their phones away when required. They will use them appropriately when permitted. They will accept that there are times when a phone is useful and times when it is simply a distraction.

The challenge is the minority who deliberately test rules and boundaries.

Every school knows that there will always be learners who attempt to circumvent restrictions. They may bring a second device, use mobile data rather than the school's network, attempt to defeat a physical restriction or simply take advantage of moments when supervision is less obvious.

But the safeguarding issue is not necessarily confined to that individual learner.

- A learner accessing inappropriate material can show it to other learners.
- A learner who creates a harmful group chat can draw others into it.
- A learner who records another learner whether appropriately or inappropriately, can distribute the recording.
- A learner who discovers a way around a restriction, can share that method with friends.

What begins as an individual breach of school policy can therefore become a wider safeguarding issue.

This is why, perhaps, the question should not simply be:

"Do our learners obey the phone policy?"

It should possibly also be:

"What happens when they don't — and how do we prevent the behaviour of a minority from exposing other learners to harm?"

There Is a Third Position

The debate about school phones can sometimes feel like tossing a coin.

On a hard, flat surface, the coin lands on either Heads or Tails. One side says: Ban the phones. The other says: Allow the phones. Much of the discussion becomes an argument about which side is right.

But a coin does not always land flat. On an uneven or softer surface — sand, grass, bush or another irregular surface — it can occasionally land on its rim.

Perhaps that is a useful way of thinking about the school phone debate.

This implies that there is a third position. It is not necessarily about banning the physical device. It is not necessarily about allowing unrestricted use. It is about managing the digital environment in which the device operates.

A school might reasonably decide that, in its school policy:

- phones are not permitted during lessons;
- phones may be permitted during breaks;
- phones may be permitted on a school hike, but must remain on silent;
- phones may be permitted on a school bus but not used while the vehicle is moving;
- phones may be used during a sports tour for communication and emergencies;
- certain applications or categories of online service may be restricted during specified periods;
- inappropriate content may not be stored on a device or shown to other learners, irrespective of where that content originally came from.

There is no universal answer. There must, however, be an answer.

The important question for every school is therefore not simply: "Do we allow phones?" It is: "Where, when, why and under what conditions do we allow phones and other connected devices?"

That is a policy question before it is a technology question.

A Policy Cannot Be the Absence of a Decision

Perhaps the greatest risk for a school is not choosing the "wrong" phone policy. It may be having no sufficiently clear policy at all.

A school that says "phones are banned" has made a decision. A school that says "phones are allowed" has made a decision. A school that says "phones may be used in these circumstances, for these purposes, and subject to these restrictions" has also made a decision.

But a school that leaves the matter ambiguous and relies on individual teachers to make up the rules as circumstances arise may be creating an entirely different problem.

Every school should have a clear, accessible and appropriately detailed policy covering mobile phones, connected devices and digital conduct. Parents and learners should be required to acknowledge that they have received, read and understood the relevant rules.

The policy should not merely say whether phones are permitted. It should address questions such as:

- Where may a learner possess a phone?
- Where may it be switched on?
- Where may it be used?
- Is it permitted in classrooms?
- What about playgrounds and break periods?
- What about school buses?
- What about sports tours, camps and excursions?
- What about boarding houses and school functions?
- What happens when a learner is under the direct supervision of a teacher away from the school campus?
- What happens when a learner uses mobile data rather than the school's Wi-Fi?
- What applications or categories of service are permitted or restricted?

- What happens if a learner deliberately circumvents the school's controls?
- What happens if inappropriate material is already stored on the device?
- What happens if a learner shows that material to another learner?
- What are the rules regarding photographing or recording other learners?
- What happens with photographs taken without consent, including inappropriate or intimate images?
- What happens if material is shared through WhatsApp, messaging, gaming or social platforms?
- What are the rules concerning gambling?
- What happens when a learner is contacted by an unknown person?
- How are suspected grooming, harassment, cyberbullying or exploitation reported?
- What may a teacher or school legitimately inspect, and under what circumstances?
- Who is responsible for dealing with an incident?
- What records should be kept?

These are not merely questions about technology. They are questions about school governance, safeguarding, responsibility and reasonable behaviour.

A signed policy does not make the school immune from responsibility. It does, however, demonstrate that the school has thought about the risk, communicated expectations and established a framework for managing foreseeable situations.

Nor should a school assume that faith, values or good intentions are a substitute for a properly considered safeguarding policy. A school may be values-driven and still need clear rules, because safeguarding exists precisely for the circumstances in which good intentions, peer pressure or individual judgement are not enough.

The hidden cost of phone policing

There is another part of the debate that deserves considerably more attention: the cost to staff.

A school can have an excellent policy on paper, but somebody has to enforce it.

- Teachers are expected to determine whether a learner is using a phone for an authorised purpose or simply browsing social media.
- They may have to confiscate devices, identify repeat offenders, deal with parents, supervise storage, return phones, investigate alleged misuse and make decisions about exceptions.
- Coaches and activity leaders may face the same issues during sport.
- Staff, and sometimes parents assisting with school trips and excursions, may face the same issues away from the normal school environment.

And then there are the awkward situations.

- What happens when a learner needs to contact a parent?
- What happens when a sports team is travelling?
- What happens when a school function finishes late?
- What happens when a learner is on a cultural or educational excursion?
- What happens when a phone is legitimately required for navigation, transport, communication or an emergency?

The more circumstances a school encounters, the more complicated the simple “phones are banned” rule becomes.

And every additional exception creates another decision for a member of staff.

The school day does not always end at the school gate!

This is particularly important when considering the school’s duty of care.

Learners may remain under school supervision during sports fixtures, tournaments, school trips, camps, cultural activities, performances, school functions and transport.

The physical location may change, but the school’s responsibility does not necessarily disappear.

Learners using their own smartphones and mobile data can operate outside the school’s Wi-Fi environment. When learners are under school supervision, the safeguarding question therefore cannot always be reduced to what is happening on the school’s network. We have examples from certain schools where parents insist their child always has their phone with them whilst on a school excursion for safety and security reasons.

This creates an obvious tension.

- A learner may legitimately need a phone during a sports trip.
- They may need to contact a parent.
- They may need transport information.
- They may need access to an emergency contact.

But the school may still have a responsibility to prevent the device from becoming a source of inappropriate content, cyberbullying or harmful activity affecting other learners.

A physical ban is therefore not always practical nor is unrestricted access necessarily appropriate.

This is where context becomes important.

From managing the device to managing digital access

Perhaps schools do not always need to manage the physical device at all.

There is an important distinction between device management and digital access management.

Device management means controlling the physical phone: confiscating it, locking it away, installing software on it or inspecting it.

Digital access management is different.

It means defining what digital services, applications and categories of content are available at a particular time, in a particular place and for a particular purpose.

For example, a school policy might state that phones may be used during specified periods for:

- contacting parents or guardians;
- educational applications;
- approved learning resources;
- navigation and transport information;
- school-approved activities;
- emergency or safeguarding purposes.

At the same time, the policy could prohibit or restrict social media, gaming, pornography, gambling, inappropriate content and other defined categories during school-controlled periods.

The technology can then help enforce the policy.

The learner still has their phone.

The school does not necessarily need to inspect the learner's private messages.

Instead, appropriate technology can restrict access to defined applications or categories during defined periods.

For example, social-media applications might be restricted during lessons but become available during an approved period. Educational applications could remain available. A school trip could have different rules from a normal classroom. A sports fixture could have another set of permissions.

The policy determines what is appropriate.

Technology helps ensure that the policy is consistently applied.

The teacher does not have to make every individual decision.

This is not the same as monitoring everything

This distinction is crucial.

There is a significant difference between filtering or restricting access to defined categories of content and monitoring a learner's private communications, keystrokes or personal messages.

The latter is substantially more intrusive, particularly when the device belongs to the learner or their parents.

Learner-owned devices carry a higher expectation of privacy, particularly outside school hours, off campus and for personal communications. Monitoring should therefore be purpose-specific, proportionate, contextually justified and time-limited.

Less intrusive alternatives can include DNS-level filtering, which can block harmful categories without accessing private messages or keystrokes and can provide category-based reporting rather than detailed records of individual browsing.

That distinction should be at the heart of any modern school policy.

Safeguarding does not automatically mean surveillance.

A school should not have to choose between doing nothing and monitoring everything.

A more practical model: contextual digital safeguarding

Perhaps the future of school smartphone policy is therefore not about whether the phone is on or off.

It is about whether the phone is being used appropriately for the context.

Consider a simple framework:

This is not necessarily more complicated for teachers. In fact, if implemented properly, it could be less complicated.

The policy establishes the boundaries.

The technology maintains them.

The staff intervene when there is a genuine concern rather than spending their time policing every phone.

Technology as digital maintenance

This may be one of the most important shifts in thinking.

Schools already maintain physical infrastructure. They maintain buildings, access-control systems, fire systems, CCTV, networks and security systems. They do not expect individual teachers to manually check every door throughout the day.

Digital safeguarding can be approached in a similar way.

Instead of expecting teachers to continually police whether a learner is accessing an inappropriate application, the school can establish the rules once and use technology to maintain those rules.

This could mean:

- restricting particular applications during specified times;
- blocking defined categories of harmful content;
- allowing approved educational applications;
- applying different policies to different age groups;
- changing restrictions for specific school activities;
- generating alerts when defined indicators of potentially concerning behaviour are detected;
- routing safeguarding alerts to the appropriate safeguarding personnel rather than simply to IT;
- maintaining an auditable record of the controls that have been applied.

The objective is not to watch everything. It is to reduce the amount of routine human intervention required to maintain a safe digital environment.

What about BYOD and privacy?

This is where schools need to exercise care. A learner's personal smartphone is not the same thing as a school-owned laptop.

Learner-owned devices are personal devices and generally carry a significant expectation of privacy, particularly outside school hours, off campus and for personal communications.

That means a school's policy should not simply assume that because a learner attends the school, everything on their personal device is available for inspection.

The school needs to establish:

- what it is trying to achieve;
- what information is actually necessary;
- what technology is being used;
- when it operates;
- what it can access;
- who can access the information;
- how long information is retained;
- what happens when the learner leaves school supervision;
- and what happens at the end of the academic term.

This is particularly important when considering intrusive monitoring of messages, keystrokes or private communications.

Use the least intrusive technology capable of achieving the legitimate safeguarding objective.

Where simple filtering or application controls can achieve the objective, there may be little justification for deeper inspection of private communications.

The goal is not to treat every learner as a suspect

There is a danger that the understandable concern about digital safeguarding leads schools towards increasingly intrusive systems.

That would be a mistake.

The majority of learners should not be treated as though they are constantly under suspicion because a minority may test the boundaries. At the same time, schools should not ignore the fact that the actions of that minority can affect others.

The answer lies somewhere between those two extremes.

Protect the majority without turning the majority into a population under surveillance.

That requires a combination of:

- clear policy;
- learner education;
- parental understanding;
- proportionate technical controls;
- appropriate supervision;
- a clear safeguarding escalation process;
- and good governance.

Technology should support those things. It should not replace them. So what should a school actually consider?

For governing bodies and school leadership teams, perhaps the starting point is a series of relatively simple questions:

1. What is our actual objective?

Are we trying to reduce classroom distraction, prevent harmful content, protect learners from cyberbullying, manage social media, address safeguarding concerns, or all of these? Different objectives may require different controls.

2. What are we currently asking teachers to police?

How much staff time is spent checking phones, confiscating devices, managing pouches, dealing with exceptions and investigating misuse?

3. What happens when learners leave the classroom?

Does the policy still work during sport, trips, camps, functions, transport and other school activities?

4. What happens when a learner uses mobile data?

Network filtering cannot necessarily address a device that is no longer using the school's network. This is particularly significant in boarding environments, where learners may use 4G/5G directly from their own devices.

5. Are we managing the device or the digital environment?

Does the school really need control of the physical phone, or can the school's legitimate objectives be achieved through appropriate digital access controls?

6. Are our controls proportionate?

Are we blocking a category of harmful activity, or are we monitoring private communications when a less intrusive solution would achieve the same objective?

7. What happens when something genuinely concerning occurs?

Who receives an alert? Who decides whether it is a safeguarding issue? What is the escalation process? And is there a clear distinction between an automated alert and an allegation requiring human assessment?

A different way of thinking about the smartphone

The smartphone is unlikely to disappear from schools. Nor should it necessarily have to.

The challenge for schools is to recognise that a smartphone is simultaneously a learning tool, a communication device, a source of distraction and a gateway to a digital world that the school cannot completely control.

The traditional response has been to take control of the physical device.

The emerging response is to take control of the digital environment.

Neither should be applied blindly.

A school that simply bans phones may find itself continually policing exceptions, confiscation and circumvention.

A school that monitors everything may create an entirely different problem around privacy, proportionality, trust and governance.

There is perhaps, another possibility.

Define the acceptable digital environment clearly, use technology to maintain those boundaries where appropriate, and reserve human intervention for the situations that genuinely require it.

That approach does not remove the school's duty of care.

It may actually make that duty more manageable.

And perhaps that is the real opportunity.

The question for schools is no longer simply:

"Should we ban phones or monitor them?"

It is:

"How can we create a safe, responsible and proportionate digital environment for our learners — while allowing our teachers to teach rather than police phones?"

That, we believe, is a conversation worth having.

Acknowledgement and Legal Context

This opinion piece is jointly authored by Dr Vincent Watters and Advocate Nicholas J Tee. Advocate Tee's contribution and insights into the practical issues facing schools have been invaluable, particularly in considering the difficult balance between learners' rights to privacy and dignity, POPIA and the safeguarding responsibilities of schools.

Advocate Tee is an Advocate of the High Court of South Africa and a member of the Johannesburg Society of Advocates. His practice includes POPIA, constitutional law and related governance matters, and he lectures on POPIA and constitutional law. The article is a jointly authored opinion piece, not a formal legal opinion or a definitive statement of how a court would decide a particular case.

The article presents the balance between privacy and safeguarding as an issue requiring careful judgement. In the discussions informing this piece, Advocate Tee has emphasised that the relevant legal questions have not yet been resolved through court decisions that provide direct, definitive guidance for every school context. This makes careful governance and context-specific judgement especially important; it does not mean that schools are without applicable legal duties. Learner-owned devices attract significant privacy considerations, and any monitoring or processing of personal information should have a lawful basis, be transparent and proportionate to the safeguarding objective. Schools should obtain their own legal advice, particularly where technologies may access personal communications, images, identifiers or other personal information.

The objective of this article is therefore not to provide a legal answer. It is to encourage school leaders to ask the right governance questions before deciding what their answer should be.

An invitation to discussion

We offer this opinion piece in the spirit of constructive debate. Schools will reach different conclusions according to their learners, communities, resources and obligations. The important starting point is that each school should understand its policy, the circumstances in which it applies, the risks it is intended to address and the safeguards that make its approach fair, transparent and proportionate.