Qoria
Europe

Student Digital Safety and Risk Mitigation

Practical strategies for school leaders and their LOPIVI Wellbeing Coordinators

qoria.es

Contents

Introduction

In an age where children embrace the digital world as an integral part of their lives, it's essential to acknowledge the potential risks they may encounter.

While the internet offers vast opportunities for learning and exploration, there are also challenges around the use of social media, chat, video and gaming apps that can lead to unwanted exposure to pornographic and violent content, bullying, grooming and other forms of online violence, all of which demand our attention.

By remaining proactive and informed, parents, educators, and policymakers can effectively address these concerns and create safer digital environments for children to thrive in.

In this article, we shine a light on some of the complexities around preventing violence against children in the online world, and discuss some of the hidden risks within the digital landscape. Additionally, we explore some proactive strategies that schools, along with their Wellbeing Coordinators, as directed by the LOPIVI legislation on the comprehensive protection of children against violence, can implement to safeguard children's online experiences and promote their overall well-being.

Section one

Where Are We Now?

The tipping point

The digital world is deeply embedded in the lives of young people, influencing how they learn and interact. Recently, advancements in AI technologies have been rapidly evolving, often surpassing the ability of schools to adapt. It's time for schools to take a firmer, more proactive stance.

Schools are at a critical juncture, facing two key challenges:

i) To foster an environment where technology is not just accepted but valued for its role in enhancing education, and

ii) to actively ensure students' safety and wellbeing in their digital lives.

Integrating emerging technologies into educational settings is complex, especially given the added responsibility of protecting students in a digital realm often devoid of robust safety measures.

A significant shift is needed for schools to not only utilise these new technologies for educational advancement but also to understand and implement them in safeguarding students' wellbeing. Emerging technologies dedicated to wellbeing can serve as crucial tools against various online risks, including violence, that children face.

Looking to the future, it's important for schools to acknowledge this new reality and incorporate it into their strategies. By doing so, they can effectively lead their communities in navigating these changes.

In 2023 schools were caught off guard

The fast-paced and often clandestine nature of digital interactions presents a formidable challenge for schools in addressing the myriad of ways in which students engage online. From social media platforms to chat applications, the breadth of online spaces where students can interact is vast, making it difficult for schools to monitor and fully comprehend the spectrum of student activities and behaviours. Additionally, the emergence of consistent new trends and digital platforms further compounds the challenge, leaving schools in a perpetual state of catch-up as they grapple with the unexpected and often concerning online behaviours among their student body.

In 2023, we saw:

The amplification of cyberbullying through AI

Children have long been victims of cyberbullying, which involves harassment, threats, or social exclusion through digital means. However, the rise of deepfake technology now means these harms have become more personalised, targeted and hyperrealistic. It has led to serious emotional distress, feelings of shame and resentment, and damage to the self-esteem of hundreds of children. For some, it even led to self-harm and suicide.

In a 2023 survey, 9.2% of Spanish pupils, said they had suffered cyberbullying.[1]

As custodians of children's physical, emotional, and social wellbeing, schools need to ask themselves how they might detect this type of incident. Important questions to address are whether students are on or off school networks, at school, or at home, and how the safeguarding systems you have in place allow for intervention before a rapid and potentially unstoppable spread occurs.

Misinformation and fake news

Children and young people encountered a significant volume of false information, rumours, and fake news online, which impacted their ability to critically evaluate the information they saw and establish informed opinions.

Geopolitical disinformation, conflict, and graphic imagery of war flooded social media, much of it tailored to influence our young people's perceptions about the state of the world and the political stance on what they saw.

40% of spanish secondary students couldn't identify fake news.[2]

While regulation of social media platforms is an ongoing challenge, schools also need to ask the critical question of the role they play in preventing this type of content from being accessed in the first place, on student devices and at home.

Concerningly, 2023 concurrently saw more teenagers also turning away from traditional media outlets in favour of social media platforms for their news consumption. This shift opened the floodgates for the influencers they follow, at best with skewed opinions or motivations or at worst lacking credibility or evidence to inform their assertions, acting as the key educator for young people in determining right from wrong when it comes to complex and nuanced world events.

1 Ministry of Education and Vocational Training 2023
2 Universidad Carlos III de Madrid (UC3M)

Online predators

023 saw predators utilising online platforms, specifically gaming platforms, to groom and exploit children in volumes never before seen. Children and young people were put at significant risk through engagement with strangers in multiplayer chats and games, often unbeknownst to their parents.

The global advocacy agency - We Protect Global Alliance - stated in their 2023 Global Threat Assessment that there was a 360% increase in self-generated child abuse material for children 7-10 years old. This begs the question - where is this occurring, and how can schools equip their parent community to better understand the very real risks to their children within their homes?

Generative AI also played a role, with reports of online predators utilising this as a tool to train, practice and role-play their future interactions with children, fine-tuning their language and messaging to more effectively influence their targets.

Safeguarding young people from those who mean them harm is not an easy feat for schools, as this often happens in places adults don't have access to, especially when they fail to understand the sense of shame attached to incidents like this and the behaviours that follow.

Research shows victims of these crimes are unlikely in early instances to self-report or ask directly for help because they fear being blamed and shamed. Schools now need to move the needle from reactive to proactive in these instances by implementing more robust digital safeguarding solutions that alert, in real-time, when a child is in harm's way. These solutions need to enable them to gain the visibility they would not otherwise have over online activities, to effectively manage the safety and wellbeing of their students.

In 2023, there was a 360% increase in self-generated child abuse material for children 7-10 years old.

We Protect Global Alliance

29%

Instagram is now the most popular news source among younger people - used by 29% of teens in 2022 - with TikTok and YouTube close behind.

Section two

What's Coming?

Online visibility and digital safeguarding of students has become a strategic imperative.

In 2023 globally:

Every
56 seconds
Qoria Monitor spotted a child at potential serious risk.

Every
4 minutes
Qoria Monitor found a child involved in potential serious cyberbullying, bullying or violent incidents.

Every
5 minutes
Qoria Monitor found a potentially vulnerable child.

The continued evolution of emerging risk reflects the challenging nature of digital environments.

As we've navigated the online world in 2023, certain patterns have surfaced, shifting and shaping the way schools need to approach student digital safeguarding. Several noteworthy trends have been identified below, which are not only prevalent now, but are expected to intensify in the next 12 months due to the rapid development of tools and technology like generative AI, data personalisation and the convergence of immersive and augmented technologies like XR (extended realities).

These trends underscore the critical need for proactive and adaptive strategies to mitigate these escalating risks effectively.

The silencing effect

School filter avoidance

Machine drift

Up-ageing

Deepfake cyberbullying

The silencing effect

The silencing effect (TSE) refers to a phenomenon of self-censorship that occurs when individuals, particularly girls and minority groups, face online harassment, trolling, or intimidation.

Across the world, we have witnessed these groups facing significant and disproportionate targeting. The amplification of harm through tailored and personal methods is expected to increase for these groups

The silencing effect is an experience many children and young people might be faced with on any given day. They are not generally forthcoming about their feelings and are also often unsure about the timing of when situations are “serious enough,” to report. It is imperative that leaders learn to quickly recognise the behaviours associated with student experiences of The silencing effect, and identify ways to intervene early to minimise negative impacts.

Consideration needs to be given to the ways staff can detect and provide opportunities for confidential reporting of online conflict and effective strategies to manage and prevent the escalation of social, emotional, psychological, or physical harm, of which this is an example.

Machine drift

Machine drift is already a growing concern for students, where algorithms and information used to build certain technology inadvertently expose young people to problematic content as they continue to engage with it.

Current research shows machine drift is a relevant and real-time concern for the modern-day student, with a recent example showing that children are just three clicks away from adult content on platforms like YouTube. Graphic content driven by geopolitical tensions has also intensified over the past year, weaponising platforms like social media.

As user-generated online content continues to grow, machine drift will escalate as an enabler in driving the influence of questionable political agendas, unhealthy trends and disinformation.

While schools must encourage and educate students on the importance of digital literacy, teaching them to analyse and question online content, so too is it imperative to consider the ways to detect and prevent inadvertent access through filtering and monitoring, essentially automating harm minimisation. Implementing technical solutions that are flexible and customisable, will allow schools to quickly get on top of new or emerging trends throughout 2024 to address the challenges posed by experiences like Machine drift.

> Machine drift is when we rely on algorithms for our searches. Allowing this drift poses risks, especially for those who can't discern reality from fake information or ignore extreme content. The greatest danger posed by artificial intelligence is the spread of misinformation and extreme content in society."

Dr Catherine Ball
Scientific Futurist

School filter avoidance and cybersecurity risk

Students attempting to bypass school filters is a tale as old as time. However, the current digital climate has evolved to not only pose greater risks to student wellbeing, but also to schools' cybersecurity posture.

2023 saw students continue attempts to access content off school networks, exposing them to deception tactics such as the utilisation of spoofed websites and impersonation accounts. The use of strategies like these by threat actors and organisations is expected to increase and evolve in 2024.

Coupled with new automation techniques and an increased volume of scam-based activity, unsuspecting young people will be more easily convinced to click on links that jeopardise their device, and subsequently their school's network's cybersecurity.

The fallout of victimisation in these instances is now causing significant reputational damage to schools that were not able to demonstrate the practical steps they had taken to effectively mitigate and manage these behaviours in current digital contexts.

This situation emphasises the advantages of managed devices in educational settings. Managed devices offer a more controlled and secure environment, significantly reducing the risks associated with unmonitored internet access and device misuse. Robust and nuanced filtering solutions and internet management tools that adapt quickly to cybersecurity requirements, coupled with education and engagement of students on the consequences of filter avoidance, are crucial considerations for

Deepfake cyberbullying

Deepfakes are synthetic media that have been digitally manipulated to replace one person's likeness convincingly with that of another. The rise of deepfake technology use among young people introduces new challenges for schools.

Cyberbullying using this type of technology escalated at the end of 2023, and despite in many instances the result constituting criminal or civil offences, it is likely to continue.

The harm caused by deep fake content, typically targeting victims by showcasing individuals in pornographic or sexual contexts, can result in severe mental health implications for victims and can have a long-term impact on a student's digital footprint.

Cases globally have also raised concerns about the duty of care and the ability of schools to create safe psychosocial environments for teachers following a spate of deep fakes created by students, targeting the teaching staff at their schools. Schools must integrate digital citizenship programs that target new and emerging trends, as well as educate students about the ethical use of technology and the consequences of harmful content creation.

Up-ageing

According to McCrindle's research, Up-ageing is defined simply as "young people growing up faster, at a younger age," and is a significant trend that

parents, and subsequently schools, are grappling with thanks to students' increased use and access to digital technologies. Parents are managing the tension of knowing their children need to develop comprehensive digital literacy when it comes to devices; however, they also understand that their children don't have the developmental skills to be careful and safe.

Many parents and schools have concerns about children growing up too quickly. Nevertheless, as technology becomes more available and important for learning, children are often left to use devices and tools without enough supervision–both at school and at home. This can expose them to inappropriate content, which without sufficient supervision, intervention, or adult engagement, kids may be negatively impacted by content unsuitable for their age.

The concept of up-ageing underscores the critical need for tools and interventions to help kids have age-appropriate digital experiences and interactions.

Schools should engage and educate parents in conversations about age-appropriate technology use, providing resources and learning opportunities to guide their communities regularly and consistently.

Teachers, in particular, must also be equipped and resourced to address behavioural consequences resulting from premature exposure in schools and to be able to effectively communicate with students on the online safety issues that affect them.

When these elements are considered and prioritised, educators can intervene and proactively detect concerns like "up-ageing" and address this in a targeted and strategic way.

Section three

Risk Mitigation Strategies Schools Can Adopt Now

Where to from here? The importance of visibility in supporting digital wellbeing.

There is a lot for schools to consider when it comes to students' use of technology, and it can, at times, feel overwhelming. Therefore it's important to remember that small and consistent steps in the right direction are what often drive the biggest impact. So, where should schools and their Wellbeing Coordinators focus their attention when there are so many areas to look at?

When it comes down to having true impact, there is 1 key focus area that will truly move the needle on improving students' outcomes. That is digital visibility.

We believe it is one of the biggest barriers to children's digital wellbeing today, and it's a very real blindspot in schools around the world.

"Visibility" is the capacity to see and understand the digital habits, behaviours, and risks experienced by children and young people. It is a crucial element of any successful digital safety and wellbeing strategy because it helps schools mitigate risk by informing preventative measures to protect and support individuals based on their specific needs.

It is good news that a vulnerable child can often be spotted through their digital behaviour.

Gaining visibility can help schools detect problems and respond to issues they were previously unaware of and help students who hadn't been shown to be at risk or struggling. By monitoring online behaviour, it is possible to identify patterns and behaviours that may negatively impact wellbeing. Increased visibility also provides greater control over a student's digital environment, fostering online safety.

A comprehensive understanding of the workings of devices and services, along with associated risks, enables clear and informed decision-making around their usage and the protection of personal information. When they have visibility, schools can transition from reactive to proactive online safeguarding practices.

Visibility is crucial in achieving digital wellbeing because:

- It helps schools negate risk by informing targeted preventative measures to protect and support individuals based on their specific needs.
- It can help identify issues, address concerns that were previously unnoticed, and assist students who hadn't been identified as at risk.
- It reduces the need for intervention down the track, by preventing issues from escalating.
- It gives schools more control over the digital environment and promotes online safety.
- It enables schools to make data-driven and well-informed decisions regarding their digital safeguarding strategies and initiatives.

> I still don't know if we as a community really understand the impacts of cyberbullying and digital citizenship and how our children are behaving online. I feel we still have a lot of work to do as a school around highlighting some of the online dangers, so we keep putting it out there and talking about this with our communities."

Brook Hill
Principal, Netherton School

Making the invisible, visible

Relying on eyes and ears only in the online world is no longer enough...

Historically, many schools have often relied upon the observations and intuition of teachers to determine who is struggling, and why. While the eyes and ears

of teachers will always be an indispensable means of spotting potentially problematic situations, it is by no means a catch-all. The ability to see what's happening inside a student's digital life is largely impossible without the aid of technology.

Additionally, relying solely on physical monitoring lacks the capability for pattern building or trend analysis. Addressing a single, seemingly minor incident may be quickly forgotten, however, the connection of multiple online actions can often unveil previously unseen dangers.

Duty of care requirements for schools to handle issues wherever and whenever they arise is omnipresent, so when students step beyond the school gates and encounter online risks, schools still need to be prepared to intervene. While observation is a crucial tool for understanding and supporting a child's wellbeing, it is not sufficient on its own.

Children often conceal their struggles, and some may not be able to recognise or articulate their concerns. Having visibility can help address this.

How can schools improve visibility?

One of the key roles of the Wellbeing Coordinator according to the LOPIVI is to maximise wellbeing at school. To improve students' wellbeing, schools need to consider how much visibility they have in three key areas: feelings, intentions, and actions.

Three key questions will also help identify gaps in provision and emphasise where a greater or enhanced focus may need to be placed.

1. How can we tell how our students are feeling regularly?

It's essential to check in consistently with students about their emotional state and wellbeing. Their perception of what's going on in their lives is a good indicator, so tracking changes in mood or behaviour can provide useful insights into their wellbeing. Having an effective methodology or system for gathering student feedback and regularly asking them how they're feeling is a good starting point for addressing any concerns and getting on top of things early.

Internationally, schools are progressively adopting focused, technology-driven approaches to gather student feedback. Specifically, they are turning to wellbeing feedback platforms and weekly check-in tools to identify and proactively support individual students and provide schools with actionable data to understand where their students are thriving and what needs work.

Analysis of over 23 million Linewize Pulse check-ins revealed that one of the main reasons for ill-being for children globally is 'concern over the mistakes they make'.

2. How do we know what they're searching for or looking at?

Understanding how students are using their school devices online can provide valuable information and patterns that showcase their intentions, interests, concerns, and potential risks. Certain types of searches can be flagged to identify patterns and behaviours that may negatively impact their wellbeing. It can also bring to light overarching trends or issues, typically on an aggregated level.

Filtering technologies have seen significant advancements over the years. However, when considering the most suitable filtering solution to gain better online visibility, schools should prioritise filters explicitly designed for educational environments. Unlike solutions created for corporate systems administrators, these education-specialised technologies offer schools the ability to allow key stakeholders, such as a wellbeing coordinator to be able to access reports. They should also be able to adjust and tailor filtering methods according to observed student behaviours. An effective filtering solution in schools should steer away from a one-size-fits-all approach and, instead, focus on adaptability, personalisation, visibility and accessibility. It should possess the flexibility to accommodate diverse learning needs of different students or year groups while safeguarding all students from potential online risks.

How can schools improve visibility? cont.

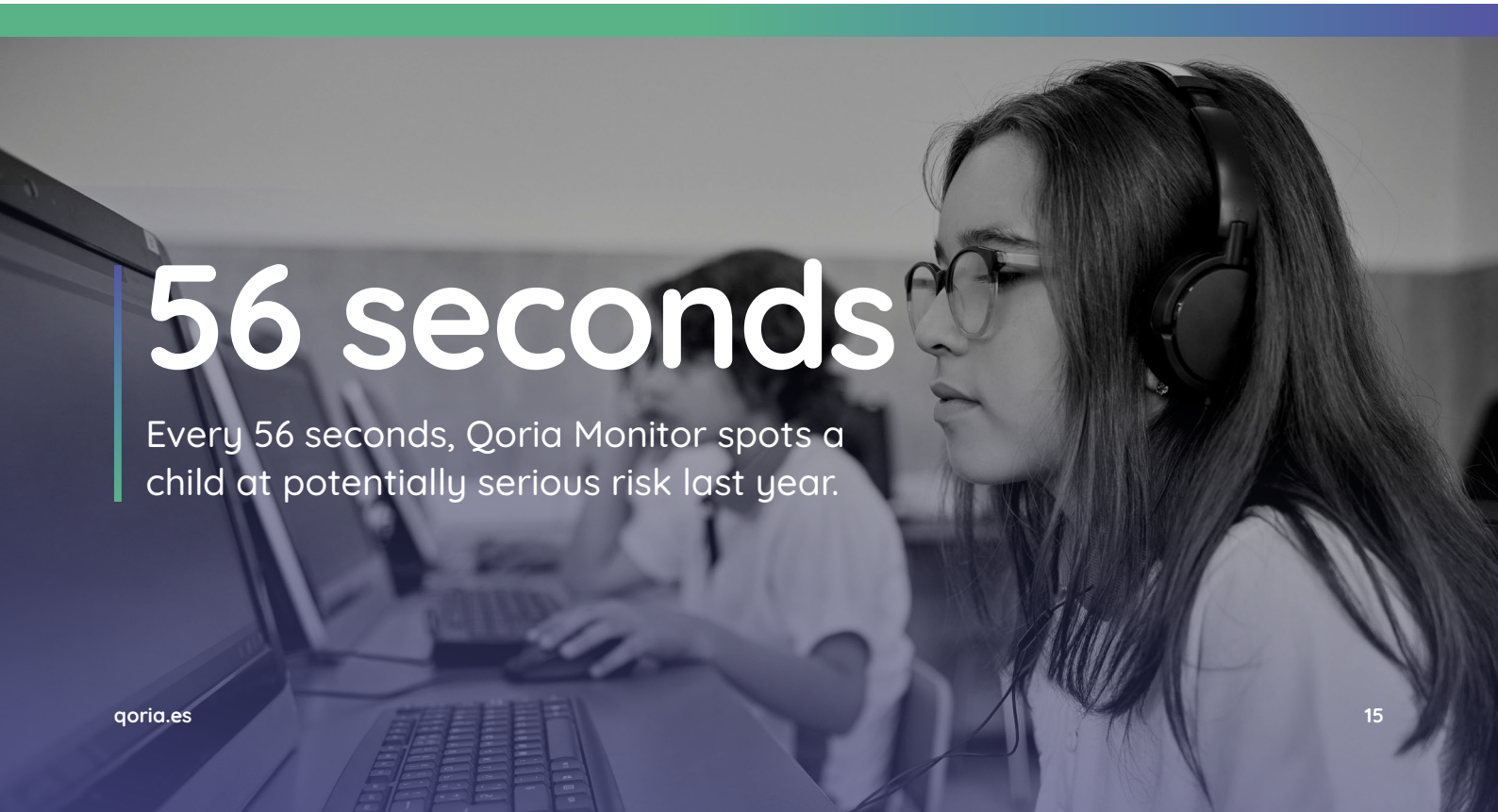
3. What are they experiencing online and encountering?

Finally, it's crucial to understand the nuanced experiences students are having online. By understanding their digital interactions and behaviours, schools can identify any potentially harmful activity, such as cyberbullying or inappropriate interactions. This insight enables the implementation of tailored preventative measures to protect and support students according to their specific needs.

As a result of the growing pace and scale of online risks, a new era in digital safeguarding has emerged with the introduction of threat detection and digital monitoring technologies. Whilst web filtering is an essential tool for shielding students from harmful and inappropriate online content, it can fall short in revealing the broader context of students' interactions.

Digital monitoring goes beyond content blocking. It categorises and alerts designated staff when a student's digital behaviour suggests they are at imminent risk of violence, and provides vital contextual information that includes causative factors.

To help schools continually comply with government regulations, we developed Qoria Monitor, a leading risk detection and monitoring solution.



56 seconds

Every 56 seconds, Qoria Monitor spots a child at potentially serious risk last year.

10 key questions schools need to ask themselves today:

In today's modern-day learning environment, ensuring the digital wellbeing of students requires a proactive and purposeful approach from schools.

To identify immediate risks and enhance visibility in the 3 key areas mentioned, schools can utilise the below set of prompts designed to encourage reflection and action.

When schools can see the gaps, they can take affirmative steps to empower themselves in safeguarding their students and to foster an environment conducive to positive and meaningful outcomes in student wellbeing.

The questions below will help identify gaps in your current digital safeguarding strategies. The purpose of this brief exercise is to assist in pinpointing and prioritising actionable areas that you can immediately concentrate on.

1. Are you using a firewall as a dedicated security solution, or are you trying to use it to block areas of the internet as well? **Y / N**
2. Can you create rules in your filter that allow you to respond directly to observed behaviours for an individual student? **Y / N**
3. Do non-technical staff receive regular reports and real-time alerts about students' digital activities? Do those reports detail behaviours, wellbeing trends, and highlight students of concern? **Y / N**
4. Do your current systems produce false positives or reports that require a lot of investigation? **Y / N**
5. Are your teachers able to determine what can and can't be accessed in their lessons when students are online? **Y / N**
6. Do you have monitoring or reporting systems that allow you to proactively identify students who are using their devices in a way that could cause them to come to harm? **Y / N**
7. Do you have a formal way of measuring and recording data on how your students are feeling regularly? **Y / N**
8. Is your cyber safety education delivered to meet the developmental age, needs, and expected digital experiences of different student cohorts? **Y / N**
9. When you run cyber safety sessions for your students, are you actively considering the learning needs of your staff in this space? **Y / N**
10. Do you have the ability to give your parents access to information about their own child's digital activity? **Y / N**

Conclusion

When we look at the digital space, your school plays an important role in mitigating violence and other risks and creating a safer online experience for your children at home, at school - and everywhere in between.

By addressing challenges through a proactive lens in the areas of preventative action, early detection and intervention, and education and engagement, schools can create a safer online environment for their students, fostering a sense of empowerment and control among all stakeholders who guide children's digital journeys.

Collaborative efforts with the right technology, tools, and experts will strengthen the collective response to the multifaceted issue of student online safety

Further reading

This article is part of our Schools Digital Safety series. Click here to visit our dedicated resources page.

Get in touch today

Whether you would like to discuss your strategy as a whole or find out more about our individual solutions please get in touch.

Contact: enquiries@qoria.es
Visit: www.qoria.es

We're here to help.

Qoria
Europe

Qoria is 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 seamlessly support them on all sides - at school, at home and everywhere in between.

Find out more
www.qoria.es