



# Student Digital Wellbeing: State of the Nation Report 2025

A report on student digital wellbeing,  
online risks, blindspots & school strategies  
for thriving in the digital era.



# Contents

<b>Introduction</b>	3
<b>Section one: Reflecting on 2024</b>	<b>5</b>
<b>Key digital risks from 2024</b>	5
Bullying through the rise of AI	5
Misinformation and fake news	6
Online predators	6
Online scams	7
Equitable access to digital literacy & consistent safeguarding	8
<b>The global rise in regulation</b>	9
<b>Section two: Preparing for 2025 - What's coming?</b>	<b>11</b>
<b>Why schools need to consider online visibility and digital safeguarding students as strategic imperatives</b>	11
1. The silencing effect	12
2. Machine drift	12
3. School filter avoidance	13
4. Deepfake cyberbullying	13
5. Up-ageing	14
<b>New insights from ySafe Cyber Safety Experts</b>	16
Student Insights	16
School Insights	17
Parent Insights	17
<b>ySafe's ABCs of online safety management</b>	18
<b>Section three: Risk mitigation strategies schools can adopt now</b>	<b>19</b>
<b>Where to from here?</b>	19
Making the invisible, visible	20
How can schools improve visibility?	21
10 key questions schools need to ask themselves today	22
<b>The Digital Safety and Wellbeing Framework</b>	23
<b>Conclusion</b>	24

# Introduction

Navigating the fast-changing world of online safety is a constant challenge for schools and their communities.

Technology is at the heart of young people's lives, offering both opportunities and obstacles. Over the past year, you've likely faced the uphill task of keeping pace with emerging apps, digital trends, and unexpected behaviours.



**As school leaders and educators, understanding these shifts and their impact on student wellbeing is more critical than ever.**

The State of the Nation is our response to this evolving landscape. Developed by global education and online safety experts, this report dives into the pressing issues affecting Australian children today and shares actionable strategies to foster a safer online environment within your school community.

The 2025 edition brings fresh insights, updated statistics, and a new section inspired by *The Next Click: What's Influencing Student Digital Behaviours and Safety in 2025*, a recent paper by our ySafe Cyber Safety Experts. Drawing on insights from conversations with over 100,000 students, staff, and parents nationwide in 2024, this report equips you with a forward-looking perspective on the digital challenges schools will face in 2025—and how to stay ahead.

Whether you're a school leader, pastoral staff member, IT professional, or simply invested in student safety, this document is essential reading. Let's prepare for what's next—together.



# 1 in 4

young people affected by  
Cyberbullying 2.0 during 2023

eSafety Commissioner

## Section one

# Reflecting on the Digital Risks From 2024

The fast-paced and often clandestine nature of digital interactions continues to pose significant challenges for schools as they strive to address the myriad of ways in which students engage online.

The digital environment has remained central to young people's lives, shaping how they learn, connect, and experience the world. 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. 2024 saw schools faced with increasing difficulties adapting to the pace of these changes and even more sophisticated digital threats, including;

### Bullying through the rise of 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.

Currently, in Australia and New Zealand, approximately 1 in 4 young people will experience cyberbullying every 12 months, and this figure is expected to continue rising (Source - eSafety Commissioner).

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 the rapid and potentially unstoppable spread occurs.

**44% of Australian young people** report having a negative online experience in the last 6 months, this includes 15% who received threats or abuse online.

## Misinformation and fake news

Children and young people continue to encounter a significant volume of false information, rumours, and fake news online, which impacts their ability to critically evaluate the information they see and establish informed opinions. Confronting, explicit, and violent imagery was viewed by young people at exponential rates, with the [Australian Bureau of Statistics](#) reporting 63% of young people have encountered potentially harmful content in the past year. While regulation of social media platforms is an ongoing challenge, schools 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, 2024 saw more teenagers 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. The proliferation of misinformation on social media has skyrocketed, highlighting the urgent need for schools to play a proactive role in educating students about media literacy and critical thinking skills to navigate the digital landscape responsibly.

## Online predators

In 2024, predators increasingly exploited online platforms, specifically gaming environments, to target and groom children. This trend placed children and young people at significant risk through interactions with strangers in multiplayer chats and games, often without parental awareness. A report by the Childlight Global Child Safety Institute found that **1 in 8 children** (302 million young people) have experienced online child abuse and exploitation in the past 12 months.

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.

Recent studies indicate that Instagram remains a popular news source among Australian teens, but its dominance is being challenged by platforms like TikTok. According to the [Digital News Report: Australia](#), both Instagram and TikTok have gained popularity as news sources for Generation Z. Notably, one in four Gen Z individuals watch news-related videos on TikTok.





### Online scams

In 2024 Australians reported losses exceeding **\$2.74 billion dollars due to scams**, and children and young people went from being collateral damage in scams to a primary target. Many fell victim to online scams, including phishing attempts, buying and selling scams through spoofing or fraudulent websites, and deceptive online strangers targeting young people with sextortion-style scams, leading to financial loss and even identity theft.

Safeguarding students from the escalating threat of online scams stands as a relatively new yet critical focus area for educational institutions. The vulnerability of young minds being misled by digital manipulation, targeted financial exploitation, or social engineering schemes is omnipresent and demands immediate proactive measures.

Addressing deceptive online behaviours ensures schools not only fulfil their duty of care, but also cultivate an environment where students can explore the digital world with increased confidence, foster critical thinking and build resilience in navigating the online landscape.



In 2024 Australians reported losses exceeding **\$2.74 billion** dollars due to scams.

### Loneliness and loss of real-world social skills

Ample research into children and young people’s behaviours indicates that in our post-pandemic world, wellbeing levels aren’t where they need to be. **Data indicates** that young people aged 12-17 had the highest proportion (3.4%) of the population seen by community mental health services, compared to younger age groups in Australia.

Loneliness continues to be regarded as being caused or exacerbated by excessive time spent online. Coupled with reduced face-to-face social interactions, the result being seen in large volumes is the negative impact on children’s development of essential communication and interpersonal skills. In 2023, the United States Surgeon General Vivek Murthy also advised that loneliness had become a **public health epidemic** causing lasting harm to physical and mental health. Dr Murthy stated that 40% of children and adolescents reported experiencing mild to moderate loneliness, and 10% felt severely alone.

Helping young people manage their time online in a balanced way both at school and at home has never been more important to help build the social and emotional capabilities they need to support their wellbeing.

## Equitable access to digital literacy & consistent safeguarding

Known in Australia as **the 28%**, or Digital Divide, these children and young people in regional and remote areas do not have equal access to online resources and opportunities due to disparities in technology availability and digital literacy education. Simultaneously, they are also **more likely** to experience online harassment, bullying, and image-based abuse than those in urban areas. Equitable education in online safety and access to technology that can safeguard students truly needs to be proactively addressed by schools so that no child falls through the gaps of the online world.

BYOD (Bring Your Own Device) programs have also been a hotly debated topic in schools. While many schools have adopted this program to recognise the essential need for digital platforms for learning, the undeniable challenges of a BYOD program have become evident as the use of technology in the classroom has evolved. Different devices mean increased breaches, which can negatively impact a student's digital and academic wellbeing. Without ongoing federal funding to support technology initiatives, schools need to consider the pros and cons of a BYOD program before implementing it.

Schools implementing BYOD programs, initially drawn to perceived benefits such as cost reduction and student familiarity with personal devices, also faced heightened cybersecurity risks in 2024. Issues like device incompatibility with school security systems, digital distractions and misuse by students, and the inability of under-resourced IT departments to ensure consistent safety parameters across diverse devices, elevated the risk of successful cyber attacks. Ransomware and malware attacks were of particular concern as students went off the network, and inadvertently exposed their accounts, devices and subsequently their schools to opportunistic cybercriminals.

## According to a recent survey,

60% of both higher and lower education providers suffered ransomware attacks in 2024 compared to 44% in 2020.

In an attempt to mitigate these risks and provide a more consistent learning experience, schools globally are starting to move away from BYOD. While this may not be an immediate possibility for some schools, it is critical that those schools focus heavily on managing their current device landscape, and when financially feasible, move toward the rollout of a 1:1 device program (where each student is provided with their own individual device for use during school hours and often for homework or study purposes).

Whatever way schools choose to manage their devices, the ability and effectiveness in closing the gaps for student safety and wellbeing should be front and centre.





## The global rise in regulation

### Escalating concerns surrounding the protection of young people's digital safety have prompted a global shift toward enhanced regulatory frameworks and digital safeguarding.

During 2024, governments and regulatory bodies have intensified their efforts to establish comprehensive guidelines reflecting a heightened recognition of the need to balance the benefits of digital connectivity with the imperative to shield young users from potential harm and privacy breaches. The below summary explores the current state of play around the world.

#### UK regulation

In the UK, the Department for Education (DfE) has introduced and continues to upgrade its statutory online safeguarding requirements for schools, specifically making monitoring an essential requirement in Keeping Children Safe in Education (KCSIE) 2024 and OFSTED. UK schools are required to have 'appropriate filters and monitoring systems in place and regularly review their effectiveness.

#### US regulation

The review of laws and regulatory restrictions like the GDPR and EU General Data Protection Regulation has prompted further tightening and focus on US online safety and advocacy laws to protect children's personal information and digital safety. To ensure compliance with laws such as the Children's Online Privacy Protection Act of 1998 (COPPA)[5] and the Children's Internet Protection Act (CIPA) [6].

Former President Biden had also issued an **executive order** to manage the responsible development of AI. This action places the highest urgency on governing the development and use of AI safely and responsibly to protect civil rights and liberties, as well as privacy.

Additionally, the Federal Trade Commission (FTC) has ramped up enforcement actions against companies that fail to comply with COPPA and other privacy regulations, signaling a more aggressive stance on children's digital safety.

#### Australian regulation

In Australia, the eSafety Commissioner implemented the Basic Online Safety Expectations (BOSE) framework which sets out clear guidelines for tech companies to apply more provisions for the proactive detection of child abuse material on their platforms and servers.

Additionally, the Australian government is moving forward with a social media ban for under-16s to protect young people from online harm. This measure aims to limit children's exposure to potentially harmful content and mitigate risks associated with online interactions. The ban is part of broader efforts to enhance online safety for young Australians and reduce the likelihood of exploitation, bullying, and other digital risks.

#### New Zealand regulation

The Department of Internal Affairs continues its review of Media and Online Content regulations to minimise the risks of harm caused by digital content to New Zealanders. The review aims to design and implement a new approach to content regulation and propose a new way to regulate providers like social media and traditional media platforms. In doing so, the exposure to harmful content will be reduced by bringing all platforms into one cohesive framework with consistent safety standards.





57%

of 12 - 17 year olds exposed  
to distressing content

eSafety Commissioner

## Section two

# Preparing for 2025 - What's coming?

Why schools need to ensure visibility and safeguarding students online are strategic imperatives. **In 2024 globally:**

Every  
**2 minutes**

we spotted a child at suspected serious risk.

Every  
**5 minutes**

we found a child suspected to be involved in a serious cyberbullying, bullying or violent incident.

Every  
**3 hours**

we found a child suspected to be involved in a serious grooming incident.

The continued evolution of emerging risks reflects the challenging nature of digital environments. As we've navigated the online world in 2024, certain patterns have surfaced, shifting and shaping how schools must approach student digital safeguarding.

Several noteworthy trends have been identified below, which were not only prevalent throughout 2024 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.

2025 is about more than keeping pace; it's about taking the lead. Being aware of current trends, allows schools the opportunity to transform the way technology is integrated into education and their communities, creating environments where students can thrive academically and emotionally while being safeguarded from harm in an ever-evolving online world.



**The silencing effect**



**School filter avoidance**



**Machine drift**



**Up-aging**



**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.

While minority groups are typically associated with TSE, it is also an experience many children and young people might be faced with on any given day. They are not often forthcoming about their feelings and are also often unsure about the timing of when situations are ‘serious enough,’ to report. Leaders must learn to quickly recognise the behaviours associated with student experiences of TSE, and identify ways to intervene early to minimise negative impacts.

Consideration needs to be given to how 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, for example.



## 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

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 2025 to address the challenges posed by experiences like Machine Drift.



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.



## School filter avoidance

**66% of higher education organisations and 63% of lower education organisations reported being targeted by ransomware in the past year.**

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' cyber security posture.

2024 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 continue into 2025. 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 device security, and subsequently their school's network.

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.

Robust and nuanced filtering solutions and internet management tools that adapt quickly to security requirements, coupled with education and engagement of students on the consequences of filter avoidance, are crucial considerations for current school communities.



## 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 continued throughout 2024, despite in many instances the result constituting criminal or civil offences.

The harm caused by deepfake 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.





3/5

students see loneliness and isolation as very challenging

## Spotlight

# Insights from ySafe Cyber Safety Experts

At the end of last year, our ySafe team spoke to over 100,000 students, staff and parents across the country to gain deeper insights into these challenges.

The findings reveal not only the scale of the issues but also the strategies that are making a difference in schools. Discover these insights in our inaugural report

[The Next Click: What's Influencing Student Digital Behaviours and Safety in 2025.](#)

Let's dive into 3 key insights:

### Student Insights

There's far more happening for our young people online than many realise. We've identified the struggles that, if prioritised, we believe would have the greatest impact on their lives and wellbeing.

#### Group chats

These seem harmless, but the perceived anonymity and invisibility when interacting online may cause some people to disclose more or act out more frequently than they would in person. We're seeing behaviours like Admins of a GC ruling with an iron fist and removing people on a whim.

We also see secondary, 'private' smaller GCs pop up, with only 'besties' invited. This can lead to whispering outside the main GC as well as exclusion and other cruel, unkind behaviour.

#### AI-powered bullying

While AI can foster creativity and learning, it also brings risks, particularly in bullying tactics. AI can generate fake photos, videos, and audio, enabling bullies to create deepfakes, fake profiles, or bots that harass victims online.

The anonymity and speed AI provides make these attacks more targeted and, in some cases, harder to trace.



## School Insights

Our experience in schools last year highlighted a key challenge, every staff member (teachers, wellbeing workers, and leaders) feels the pressure to help families navigate the digital environment and its consequences, with little time and knowledge.

### School/parent partnership

Parents and schools often have differing expectations regarding the handling of online safety education and incidents. Schools have reported a trend of decreasing parental involvement and increasing parental expectations for schools to resolve all cyber-related issues. This disconnect can lead to delays in addressing problems effectively.

### Cringe conversations

Wellbeing staff often find it challenging to connect with young people due to a lack of understanding regarding current trends. This disconnect can create awkward moments when adults attempt to be 'cool' but miss the mark, discouraging meaningful conversations. Creating connections through meaningful conversations helps build a strong foundation for trust and rapport in the eyes of young people, which is especially important when they need to seek advice or support with cyber-related issues.

## Parent Insights

Our experience with schools that seek to do more to support the children in their care when it comes to the online space is asking us to regularly engage with their parents and carers to ensure they have the insights, strategies, and answers to deal with issues at home.

### App paralysis

Children access a large number of sites and platforms every day. It is estimated that the average child accesses nearly 50 apps per week, and the apps used change over time. It is not practical or realistic to expect parents to understand or configure parental settings on all of these apps. Understanding the latest trending apps used by young people of all ages can be challenging and overwhelming for parents. This lack of knowledge prevents them from effectively supporting their children in navigating online spaces safely. As a result, parents may impose fewer restrictions than necessary, leading to increased online safety risks for their children.

### Supervision vs. surveillance

Both schools and parents often find it challenging to balance the right level of supervision and monitoring for young people. Common questions include "Should I log into my child's YouTube or Snapchat account to see who they are talking to, what they are saying, or what they are watching?" or "Should I let my child know I can see their messages?" Our advice is that visibility is essential, but so is trust.

Balancing the right level of supervision with the right level of trust is not an easy task and is made even more complex by the ability of young people to freely access content or talk to strangers, especially when much of it can disappear. Phew!



## ySafe's ABCs of online safety management

A tried and trusted framework to tackle any digital safety concern

Navigating students' use of technology and online interactions presents schools with numerous challenges, which can often feel overwhelming. However, it's important to remember that small, consistent steps in the right direction usually drive the biggest impact.

As we mentioned at the start of this paper, digital safety challenges are always evolving. Today's issues will differ from tomorrow's, with new platforms, trends, and threats emerging every year. But there's one thing that can remain constant: your approach.

ySafe's ABC framework is designed to help you tackle any digital safety concern head-on. It empowers school staff and parents to take control of online safety through three actionable steps:

1. Manage **Access**,
2. Set **Boundaries**,
3. Openly **Communicate**.

This framework has been successfully implemented by every ySafe school we partner with, and it delivers results.

[Discover how it works by downloading the full report.](#)

## 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 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 – visibility of children's online interactions (what they do, say, or share online, and with whom). 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 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 such as searches and interactions, 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.

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

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.



It's really challenging to get visibility on what happens online with your students. These things are happening in a place you don't have access to. This means you spend so much time trying to find out 'things', and often don't get the opportunity to act appropriately and help the student. With Linewize Monitor, we can."

**Derek Champion**  
Acting Deputy Head Pastoral Care Shore 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.



Keeping our students safe and protected has become harder with the increase and prevalence of technology, so we need to be upskilled and informed as best we can, to come from a place of knowledge to help our young people."

**Carrie Scanlan, Director of Students**  
Kincoppal-Rose Bay, ySafe Partner School

## How can schools improve visibility?

To improve students' digital 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 28 million Linewize Pulse data points reveals 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 what students are searching for online can provide valuable information and patterns that showcase their intentions, interests, concerns, and potential risks. Tracking searches can 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 spaces, these education-specialised technologies offer schools the crucial ability 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 and personalisation. It should possess the flexibility to accommodate diverse learning needs while safeguarding students from potential online risks.

**24 million children are supported and protected by our technologies around the world, every day.**

### 3. What are they experiencing online and encountering?

Finally, it's crucial to understand the nuanced experiences students are having online. By tracking their digital interactions and behaviour, 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 risk, and provides vital contextual information that includes causative factors.

To help schools in the UK, and globally, continually comply with government regulations, we developed Linewize Monitor, a leading risk detection and monitoring solution.

**Every 2 minutes, Linewize Monitor spotted 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

---

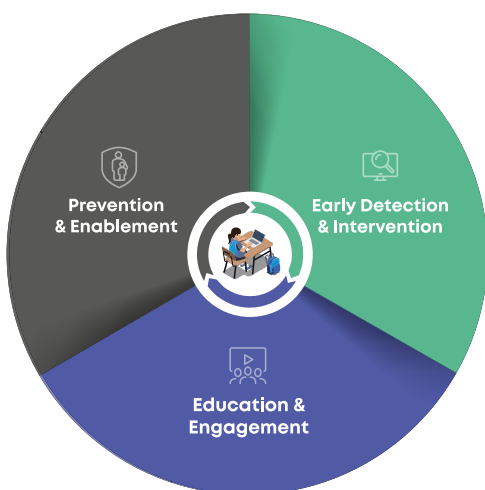
10. Do you have the ability to give your parents access to information about their own child’s digital activity? Y / N

# The Digital Safety & Wellbeing Framework

Success is in the application of new knowledge to address new problems. **Application turns knowledge into a tool and having the right tools is where schools build real-world solutions.**

As shared in this white paper, the dynamic landscape of digital safety and wellbeing demands continuous adaptation and the journey for schools toward meaningful and effective digital safeguarding doesn't just require new knowledge; it requires application. Having gained insight into the prominent trends and risks seen by global online safety experts, schools now need to turn their attention to the strategic efficacy of the solutions they have currently implemented and assess where the gaps remain.

Linewize is here to help schools and their communities effectively navigate these changes and provide solutions that fit the needs of each individual school. We do this with **The Linewize Digital Safety and Wellbeing Framework**, which is designed to empower school leaders with the insights and solutions necessary to address their unique needs as they apply to the three most common pillars in a digital safety and wellbeing strategy.



**Prevention | Intervention | Education**

The framework addresses the pressing need for greater visibility in students' offline and online lives. By utilising this comprehensive framework, schools can assess their current strategies and prioritise action areas where more visibility is needed for targeted support, allowing the implementation of proactive interventions that elevate the overall wellbeing of their students.

The right information. Right people. Right time.

Each pillar addresses the key components of an effective digital safety and wellbeing strategy.

- Schools can leverage this framework, backed by our team of experts, to pinpoint their priorities and strategically plan the necessary steps for establishing a more effective, dynamic, and resilient digital wellbeing and safeguarding plan over time.
- Our framework also serves as a practical solution for school leaders to stay informed about the various opportunities offered in the market.
- The framework empowers schools to gain a deeper understanding of both the individual and collective roles they play and how these roles work together to cultivate an effective digital wellbeing culture across the entire community.

But more importantly, for each gap in the framework that your school can address, a more comprehensive view of each child's wellbeing emerges, providing valuable insights to the entire community.

# Conclusion

When we look at the digital space, your school plays an important role in mitigating 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.

## 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@linewize.io](mailto:enquiries@linewize.io)

**Visit:** [www.linewize.io](http://www.linewize.io)

We're here to help.





### About Linewize

We combine digital safeguarding technology, child psychology expertise, in-depth educational material and awareness initiatives to help schools build positive digital cultures – where students can thrive. Linewize solutions are constantly evolving to meet the requirements of global regulations and guidelines while ensuring schools’ unique requirements.

**Find out more [www.linewize.io](http://www.linewize.io)**  
**Email:** [enquiries@linewize.io](mailto:enquiries@linewize.io)



### About Qoria

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

**Find out more [www.qoria.com](http://www.qoria.com)**