Linewize Insights

Everything You Need to Know About Digital Safeguarding Technology

A Guide for Schools

Helping New Zealand schools better understand Digital Safeguarding Technology and the role it plays in your wellbeing programs.

linewize.co.nz

Linewize by Qoria

Contents

Introduction

This document has been produced by Linewize's experts to help your school better understand Digital Safeguarding Technology and the **role it plays in your wellbeing programs.**

Schools across the UK and USA are deploying Digital Safeguarding Technology at pace to address the postpandemic digital risks students face and minimise the subsequent impact on their mental health and learning.

Linewize's Digital Safeguarding Technology is called Linewize Monitor. It is a multi-award-winning solution that protects over a million students across the UK and US. It is the first technology of its kind to be available to schools across New Zealand.

If you have any questions or would like to see a demo please do not hesitate to contact the Linewize team at: www.linewize.co.nz/contact

This guide is essential reading for: Principals, senior leadership teams, wellbeing leaders, governors, IT and anyone interested in or responsible for digital safety and wellbeing in a school.

Why The Need For New Technology

There has always been a need for Digital Safeguarding Technology.

What a student says, does, or shares in their digital life can expose them to harm or reveal other concerns they may be experiencing. Because a child's digital world is commonly off-limits to their responsible adults, these risks slip under the radar and school leaders and parents are powerless to intervene.

The four challenges we currently face

There are four major changes impacting student safety and wellbeing.

1
A rise in online risk and dangers to children.

2
Children are spending more time online than ever before.

3
Parents are now recognising the risks.

4
Parents are ill-equipped to deal with it by themselves.

Historical approaches to student digital safety saw schools take care of device filtering during the day and parents take over via parental control apps in the evenings.

Linewize research shows that over 50% of parents do not engage with their apps, leaving significant volumes of students unprotected out of school hours.

This hard division of accountability and giving parents DIY tools to go it alone are not working. It's becoming an outdated concept in favour of more flexible arrangements tailored to parents' differing needs and circumstances.

A rise in online risk and dangers to children

Digital devices kept many children socially and emotionally connected during lockdown but it also pushed their daily lives online. This gave rise to an increase in concerning online behaviours and external risks that continue today. These include gaming addiction, online bullying, and social media addiction, to name a few.

Children are spending more time online than ever before

Children are spending more time online, and this increase shows no sign of abating. A recent survey[1] reveals that before the pandemic, parents were concerned about the amount of time their children were spending online. And since lockdowns have ended, the situation is far worse.

It is generally accepted that the increased time spent online will likely have a significant impact on their mental health.

Parents are now recognising the risks

A recent survey of some 9,000 parents across 20 countries shows that 84% of parents worldwide are now worried about their children's onlinesafety[2]. And that is one of their most prominent concerns. The same research showed that parents acknowledge they need to provide their children with more guidance, but don't feel confident doing so.

Parents are ill-equipped to deal with it by themselves

Notwithstanding their recognition of the dangers, parents and caregivers still feel they lack the knowledge and skills to help their children. They are being asked to support their children's online awareness and education, or assist with onlinerelated problems, while often knowing less than their children and while juggling demands from work and economic circumstances.

[1] Pew Research
[2] Kaspersky

The Iceberg Effect

When it comes to addressing any of these challenges, there is a major hindering factor: **the cloak of invisibility.**

When a student steps into harm's way or becomes vulnerable online there can be clues staff or parents can see with eyes and ears alone: changes in mood or appearance, or sudden deterioration in academic performance, for example.

However, there are many more clues inside the child's digital world that parents and schools have little, if any, access to, and which are therefore impossible to see.

What children do, say or share online and to whom can place them in harm's way.

It can also indicate the emergence of early stage risk and behavioural patterns that, without intervention,could escalate into something far more serious. Their behaviours can also reveal vulnerabilities in other areas of their lives. Mental health concerns or suicidal ideation are often discussed with friends in online forums, or feelings can be expressed in a document and then quickly deleted.

We call this 'see/can't see' phenomenon the Iceberg Effect. We believe it is one of the biggest barriers to child digital wellbeing and it's a very real blind spot in schools across New Zealand.

Offline risks
you can see

Changes in behaviour. Injuries/bruises, tip offs from peers, absenteeism.

Digital risks
you can't see

Online bullying or conversations about drugs/ extremism/being harmed, hidden bruises/injuries, unspoken negative feelings and thoughts.

Making Invisible Risks, Visible

There are two ways for schools to make invisible digital risks visible.

1. Eyes and ears only; and

2. Eyes and ears plus Digital Safeguarding Technology.

Eyes and Ears Only

Many schools rely on the eyes, ears and intuition of teachers to determine safe online behaviours amongst students.

Though this is vital, the idea that staff can physically supervise pupils' onscreen activity is not straightforward and brings unique challenges. the cloak of invisibility.

Pupils quickly shut down inappropriate content or conversations when a staff member walks by. That means all screens must be visible to teaching staff simultaneously.

To minimise the number of supervisory staff (and therefore cost), desks must be strategically placed to ensure maximum screen visibility from one vantage point. This precludes round and L-shaped desk formations. This may be impractical in many settings. In the case of tablet devices, physical supervision, unless standing next to the student, is extremely difficult.

It may be concluded that in almost any scenario, it is not possible to properly monitor groups of students with devices using physical supervision alone.

Furthermore, physical monitoring does not easily facilitate pattern building or trends analysis. One minor incident spotted and addressed can be quickly forgotten. But a joining up of seemingly innocent online actions can reveal hitherto invisible dangers. For example, separate online searches or conversations about healthy eating, exercise and cotton wool may be of little, if any, concern. But viewed holistically can indicate a desire for information on appetite suppressants and which could suggest an eating disorder early stage or otherwise.

Eyes and Ears Only cont.

Additionally, students moving from room to room during the school day necessitates robust handovers between supervising staff or some form of online incident logging to map such trends. Both have a high potential for error or being forgotten about altogether in a busy working day — despite best intentions.

The pros

- If an issue arises, the teacher is there to deal with it immediately.
- It's an opportunity to inform the student of the risks as they occur, as well as other class members where appropriate.

The cons

- Watching every screen in a class can be resource intensive and usually requires additional classroom support staff.
- Even with additional classroom staff, it can still be difficult to see what's happening on all screens all of the time. Students often adapt screen behaviour when a teacher walks by.
- Desks should be placed within line of sight of the teacher or assistant. L-shaped desks that obscure screen visibility, for example, should be avoided.
- It is ineffective on remote devices outside of the classroom.
- Concluding that a school is 'low risk' without the aid of digital monitoring to see what's happening online could leave students in harm's way, and allow events to escalate.

> ...the idea that staff can physically supervise pupils' onscreen activity is not straightforward.

Digital Safeguarding Technology

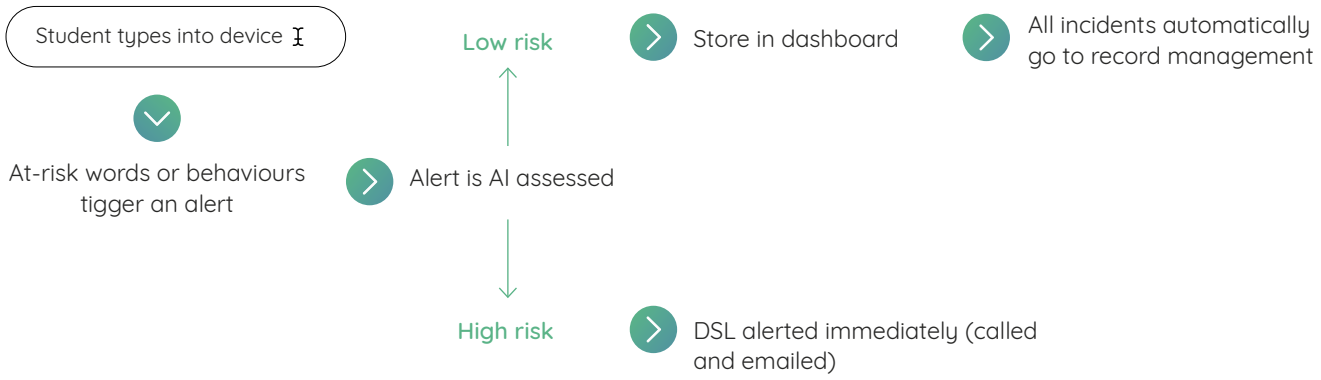
Digital Safeguarding Technology sits on any school device and alerts wellbeing staff to any student suspected to be at risk, based on what they do, say or share in their digital lives.

Serious risks such as suicide, grooming, or a gang meeting can all be picked up in real time if a child has used their keyboard in any way to view content, message someone, look for information, or type out their feelings – even if they delete it immediately or never press 'send' or 'enter'.

It can help you detect problems and respond to issues you were previously unaware of, and help individuals who haven't previously been shown to be at risk. For students already at risk you can check for escalation and feedback the evidence to relevant bodies. Active monitoring creates a safety-net for teachers who, in a busy classroom, may be unable to see what is happening online.

An alert is first checked by AI to determine if it's a false positive. If yes, no action is taken. If no, the alert is graded for severity. Low level alerts are logged in a dashboard for the school to view next time they log in. Higher level alerts are passed to a team of highly trained human moderators. They review the evidence and decide next steps. If the alert is deemed potentially serious, the school will be emailed immediately. If the alert is deemed to be very serious, including a risk to someone's health or life, the school will be contacted by phone. **All this occurs in real time and within minutes of the risk happening.**

How it works



Digital Safeguarding Technology

The pros

- It helps prevent at-risk students from going unnoticed or noticed too late.
- Students are protected 24/7, 365 days a year.
- It reveals inappropriate online behaviours to inform targeted education and awareness and encourage mental resilience among students.
- It saves the cost and administrative burden of employing dedicated teams to review risks.
- It saves valuable wellbeing time allowing them to focus on intervention and strategy, not administration.
- It is a highly effective solution to the problem of invisible digital risk, used by schools across the US and UK and currently protecting over a million students.
- It requires minimal input from IT staff.

The cons

- There is a cost associated with it.

Implementation

Digital Safeguarding Technology is quick and easy to deploy and requires very little by way of IT support once installed. The school's own IT team will access a central portal before deploying an agent onto each school device. The school's wellbeing team are trained on the system which takes around 15 minutes. They will access the portal to review alerts thereafter and of course receive more serious alerts directly via email or phone. The whole process end-to-end can be completed in an afternoon.

Frequently Asked Questions

Definitions and use

Q1: What's the difference between web filtering and digital safeguarding?

Where filtering blocks students from accessing inappropriate web content, digital safeguarding detects risks based on keystrokes - regardless of whether they are on the internet or any digital document.

For example, a web filter would block access to a site containing pornography but wouldn't detect a child having an inappropriate conversation with an adult in a chat room, whereas Digital Safeguarding Technology would. Web filtering and safeguarding technology work hand-in-hand to provide a comprehensive digital safety strategy.

Q2: We receive safety alerts from our web filter, what's the difference?

Filter alerts are usually only based on search terms used in a web browser — not on activity that happens within a website already accessed, or within any other digital document.

Filter alerts are not human-moderated and do not provide context-based analysis, including any screenshots that may show intent. Nor do they alert you to any risks shown by keystroke activity within non-browser apps such as Microsoft Word, PowerPoint or Teams.

Q3: What does real-time digital safeguarding mean?

Real-time digital safeguarding refers to the action of capturing and alerting a school to a risk as soon as it happens. This allows wellbeing teams or nominated staff members to intervene at the earliest point and deliver appropriate support.

It also enables wellbeing staff to understand any key trends in online behaviour among students, which can then be used in a timely manner to inform and educate specific year groups, or on a whole-school level. For example, if a previously unknown and dangerous website begins trending, or an inappropriate image is being shared, schoolwide communication can happen the same day if required.

Q4: What does human moderation mean?

Human moderation refers to a team of analysts who grade and decide on the severity of any alerts captured by a digital safeguarding solution. When a risk level is very high, the school's nominated staff member is immediately contacted by email or phone. Lower-level alerts are sent to the monitoring portal for staff to view and manage later. Human moderators also remove any further false positives which Artificial Intelligence (AI) alone may not have picked up. This saves staff valuable time not having to trawl through alerts.

Linewize's Moderators work around the clock 24/7/365, to ensure schools are immediately notified of any urgent concerns or risks to life. This gives schools peace of mind that should a student be in danger they will be informed immediately.

Definitions and use

Q5: Does it work if a device is offline?

Digital Safeguarding Technology works offline as well as online. This means if a child takes home a school device but isn't connected to the internet, the device will continue to be monitored, capturing screenshots and keystrokes. As soon as an internet connection is re-established, the system will send any data through to the moderators to analyse.

Q6: Is Digital Safeguarding Technology more appropriate for older pupils?

No. Digital safety is not just a secondary school or college concern. 19% of all serious risks detected by Linewize Monitor in 2020 were among primary school children. These are children facing a risk who could have gone unnoticed or noticed too late. If a child has a digital life, they need protection.

Q7: How much information can moderators see on a student?

Linewize's Moderators can see what the student has typed and screenshots of what they have viewed which resulted in the alert. Alongside this, moderators also have access to a limited amount of information including the student's username (which in most cases is not the student's real name, in the interest of privacy), and your organisation type, whether that be primary or secondary, for example. Should a moderator need to escalate a concern, only then will they be able to view the chosen contact information you have provided.

Frequently Asked Questions

Resourcing

Q1: How much does Digital Safeguarding Technology cost?

The price will vary depending on the number of students. Please contact us for a no-obligation quotation at linewize.co.nz/contact.

Q2: Is it possible to trial Digital Safeguarding Technology before committing?

Yes. With the growth in online dangers it is vital that schools understand Digital Safeguarding Technology and are able to make informed decisions. For this reason, Linewize makes our full moderated solution available free of charge for a period of time. This allows us to monitor your pupils 24/7 while your school, particularly your wellbeing teams, learn about the technology firsthand, in their own live settings.

For more information please contact us at linewize.co.nz/contact.

Q3: Our wellbeing team is already overstretched. Won't Digital Safeguarding Technology add to their workload?

No. Digital Safeguarding Technology, its AI capability, and the team of human moderators do all the sifting and grading of alerts so you don't have to. Anything requiring your school's attention will be shared with you as fast as possible. Full contextual analysis is also provided so the wellbeing team can respond promptly and appropriately. It is a time optimiser, not a timewaster.

Appendix

Appendix i. For more information

If you have any questions, would like to see a live demo of Digital Safeguarding Technology or to enquire about our free trial please contact us.

We're waiting to help.

Contact us at:
Web: linewize.co.nz/contact
Email: sales@linewize.co.nz

Appendix ii. Further reading

If you are interested in learning more about safeguarding technology we have prepared a series of articles.

How to make invisible digital risks visible
An essential guide for New Zealand Schools.

Appendix iii. About Linewize

We empower school communities to guide students towards safe and positive behaviours in their digital lives. When students know how to stay digitally safe and well, their confidence grows, their resilience increases and learning improves.

We combine safeguarding technology, child psychology expertise, in-depth educational material and awareness initiatives to help schools build positive digital cultures - where students can thrive.

As the digital landscape has evolved, so have we. From our humble beginnings in user authentication and content filtering we're now part of one of the biggest digital safety and wellbeing providers in the world. 23,000 schools and 12 million students rely on our technologies and educational programs everyday. Our goal is to work together to save and better children's lives; empower parents; deliver for tomorrow's educators and to be a key influencer in digital safety globally

Appendix

Appendix iii. About Linewize

Digital Safeguard Technology - Linewize Monitor

Linewize Monitor protects over a million students in the UK and US and is the first Digital Safeguarding tool of its kind to be available to schools in New Zealand. It alerts schools to any student whose digital behaviours are putting them at risk, or indicating a risk in other areas of their lives.

A combination of technology and highly trained human moderators enable schools to intervene quickly and appropriately and, if needed, initiate better awareness and understanding around what students do, say or share, moving forward. Monitor enhances lives. It even saves lives. Such is its impact, schools across the USA and UK are rolling it out at pace, as part of their digital wellbeing and culture building initiatives.

Linewize Education and Wellbeing

Linewize Education and Wellbeing programs help whole school communities to better understand digital risks. Online hubs, staff portals, parental webinars and apps - all created and curated by clinical child and adolescent psychologists, wellness experts, ex-police officers and teachers - combine to improve recognition and knowledge.

Linewize by Qoria

Linewize is a unique response to the challenge of today's connected learning environments, supporting the integration of technology, education and engagement to create cyber safe communities where students thrive.

Web: www.linewize.co.nz
Email: sales@linewize.co.nz

Qoria

Smoothwall 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