Linewize
by Qoria



The 3 B's of Digital Safety

A guide for New Zealand Schools

The online safety schools have in place for students generally falls into one of three categories. **Basic, Better, Best.** Understanding these categories will help your school understand if your current solutions are robust enough. And if not, what steps you can take.

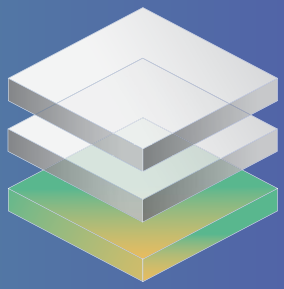
linewize.co.nz

Digital safety is not only about protecting the safety and wellbeing of students online but enabling them to use technology in a way that enhances their learning.

This guide will help your school create a roadmap toward stronger digital safety and where to allocate resources in a way that will have the greatest impact on digital safeguarding and learning outcomes.

Basic

Basic protection involves blocking harmful or inappropriate websites in their entirety, typically through a firewall or free/low-cost filtering tool.



What it means for schools

For schools, this is the most straightforward and budget-friendly approach. While this provides a first line of defence, it does not address the full range of online risks that students face today. Firewalls can block known harmful websites, but new content is emerging every second and they generally lack the flexibility that schools need to make changes on the fly to their filtering requirements. There is a significant time lag between harmful content going live and the firewall's ability to recognise and block it - leaving children exposed to risk. It's not uncommon for children who come across inappropriate content to share it amongst their friends - exacerbating the risk.

Advantages

+ **Low cost** – Affordable and accessible for schools with limited resources.
+ **Simple implementation** – Easy to set up with minimal changes to infrastructure.
+ **Basic safety** – Blocks explicit and harmful content.

The Basic level is a first step towards safeguarding children but it falls well short of the level of protection needed in today's digital landscape.

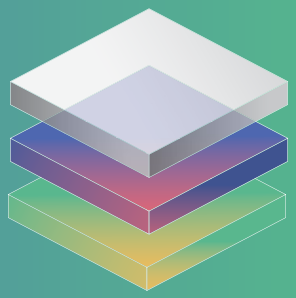
Disadvantages

+ **Limited scope** – Cannot detect risks within 'safe' websites, apps, or social media.
+ **Lag in updates** – Newly launched websites may take time to be identified and blocked.
+ **Lack of visibility** – Schools can see attempted website access but not student activity in social media, collaborative platforms, or apps.
+ **False sense of security** – Schools may assume students are safe, but filtering alone does not address cyberbullying, inappropriate interactions, or deeper behavioural risks.



Better

Schools with a better level of protection can proactively identify and block harmful content as it appears. The combination of real-time, content-aware filtering, immediate alerts, and human-moderated digital monitoring provides schools with deeper insights into risks and their origins. This enables more effective interventions and reduces the potential for escalation.



What it means for schools

At the Better level, digital safety provision is no longer a tick-in-a-box exercise but becomes more embedded in the school culture. The scope of risk detection is much wider now and takes into account student searches, app usage, and online interactions as well as deeper visibility into supposedly safe platforms like YouTube, Google Docs, email and Microsoft Teams.

Advantages

+ **Proactive risk identification** – Detects risky behaviour, not just blocked websites.
+ **Real-time monitoring** – Provides insight into students' app use, videos watched, social media interactions, and collaborative tools.
+ **Content-aware filtering** – Blurs or blocks inappropriate images and ads, even on generally 'safe' sites.
+ **Improved insights** – More detailed reporting helps schools understand and address online behaviour.
+ **Less pressure on IT teams** – Teachers and staff gain visibility, reducing IT workload and minimising alert fatigue.

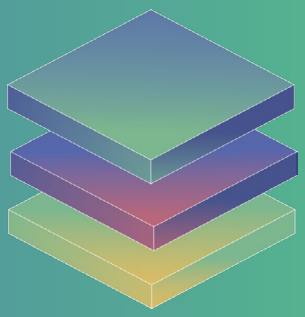
Disadvantages

+ **Higher cost** – Requires paid filtering and monitoring tools.
+ **Increased complexity** – Schools need training, policies, and procedures for managing incidents.
+ **Limited beyond school grounds** – Protection is strongest inside school networks. To extend safety at home, parent engagement is crucial.

This level enables a proactive approach—detecting risks rather than just blocking content. It allows schools to intervene before students are harmed, rather than assuming that blocking some of the internet keeps them safe.

Best

The Best provision sees the responsibility for digital safety shared across the school community, including IT teams, teachers, and parents. It ensures that students are protected on any network, on any device, at any time, at school and at home - as well as supporting teachers in managing distractions in the classroom. Best provision sees a level of protection far more aligned to the digital risks we see today.



What it means for schools

Implementing this level of digital safety requires a whole-school approach that integrates advanced filtering, real-time monitoring, and classroom management tools. IT teams deploy and maintain a unified platform, while teachers gain the tools needed to manage student device use and respond to risks as they arise. Beyond the classroom, parents are provided with similar tools to ensure consistent digital safety at home. This approach requires investment in technology, training, and clear policies to ensure its effectiveness.

Advantages

+ **Complete visibility** – Schools, teachers, and parents gain full insight into students' online activities across all devices, apps, and accounts.
+ **Real-time internet device control** – Teachers can manage student devices during lessons, reducing distractions.
+ **Integrated approach** – Protection extends beyond the classroom, ensuring consistent support at home.
+ **Increased confidence** – A sophisticated filtering system ensures harmful content and distractions are blocked without restricting learning.
+ **Better academic focus** – Teachers can immediately address digital distractions to keep students engaged.
+ **Reduced risk of external issues affecting learning** – Parents are empowered to manage digital safety, reducing problems that start outside school hours.

Disadvantages

+ **Higher cost** – Comprehensive protection requires greater investment.
+ **More involved implementation** – Setting up and maintaining an advanced system requires training and ongoing management.
+ **Privacy concerns** – Students may feel their digital activity is overly monitored.
+ **Requires more time and resource** – Requires dedicated staff to manage policies, updates, and engagement with parents.

This level of protection ensures that digital safety is not just an IT responsibility but a collaborative effort involving teachers, students, and parents. It offers the most effective protection while enabling students to thrive academically and navigate the digital world with confidence and resilience.

A quick check-up on your school's digital safety approach

10 key questions schools need to ask themselves today:

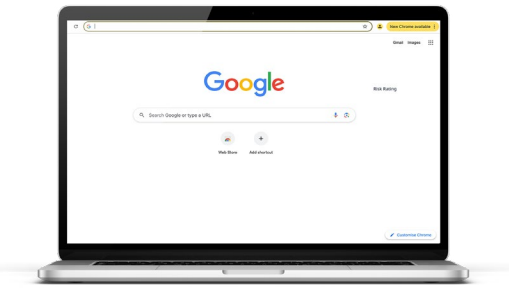
The questions below will help identify gaps in your current digital safeguarding strategies. The purpose of this brief exercise is to assist in pinpointing and prioritising actionable areas that you can immediately concentrate on.

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. Can your teachers see and control what students are doing on their devices during lessons to ensure safe and effective use? **Y / N**
8. Do you receive alerts when students engage in online activities that could put them or others at risk? **Y / N**
9. Does your filtering system reliably prevent students from accessing harmful or distracting content? **Y / N**
10. Do you have the tools to support parents in managing online challenges that arise at home? **Y / N**

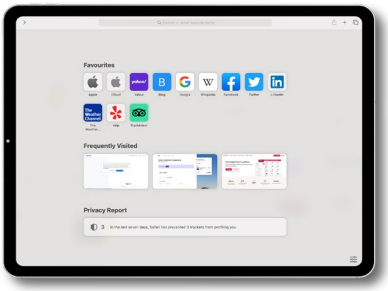


Safe Search Challenge:
Testing Your School Web Filter

Put your filtering to the test: Take the Safe Search challenge
With new online content constantly emerging, it's essential to ensure your school's digital safety measures are always up to date. To help you stay on top of this, we've created a simple way to check regularly: the Safe Search Challenge. Take the test below:



or



Chromebooks

1. Grab a school Chromebook and log into a student test account.
2. Open the Chrome browser.
3. Search Google for something you wouldn't want your students to access (e.g. age-inappropriate YouTube, Gaming, social media, adult content or explicit terms).

iPads

1. Grab a school iPad and log into a student test account.
2. Open the Safari browser.
3. Search Google via the Safari browser for something you wouldn't want your students to access (e.g. age-inappropriate YouTube, Gaming, social media, adult content or explicit terms).

This test might feel uncomfortable, but it's the most effective way to assess your filtering system. See what you discover and can access.



Where to from here?

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

The risks are real, complex, and growing. Like many New Zealand schools, you might be looking for better ways to protect your tamariki online. If you'd like to chat about what's working, what's not, and how we can help, we're here. Simply reach out—we'd love to hear from you.

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.co.nz
Visit: www.linewize.co.nz

We're here to help.

Raising the bar in student digital wellbeing together.

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: enquiries@linewize.co.nz

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