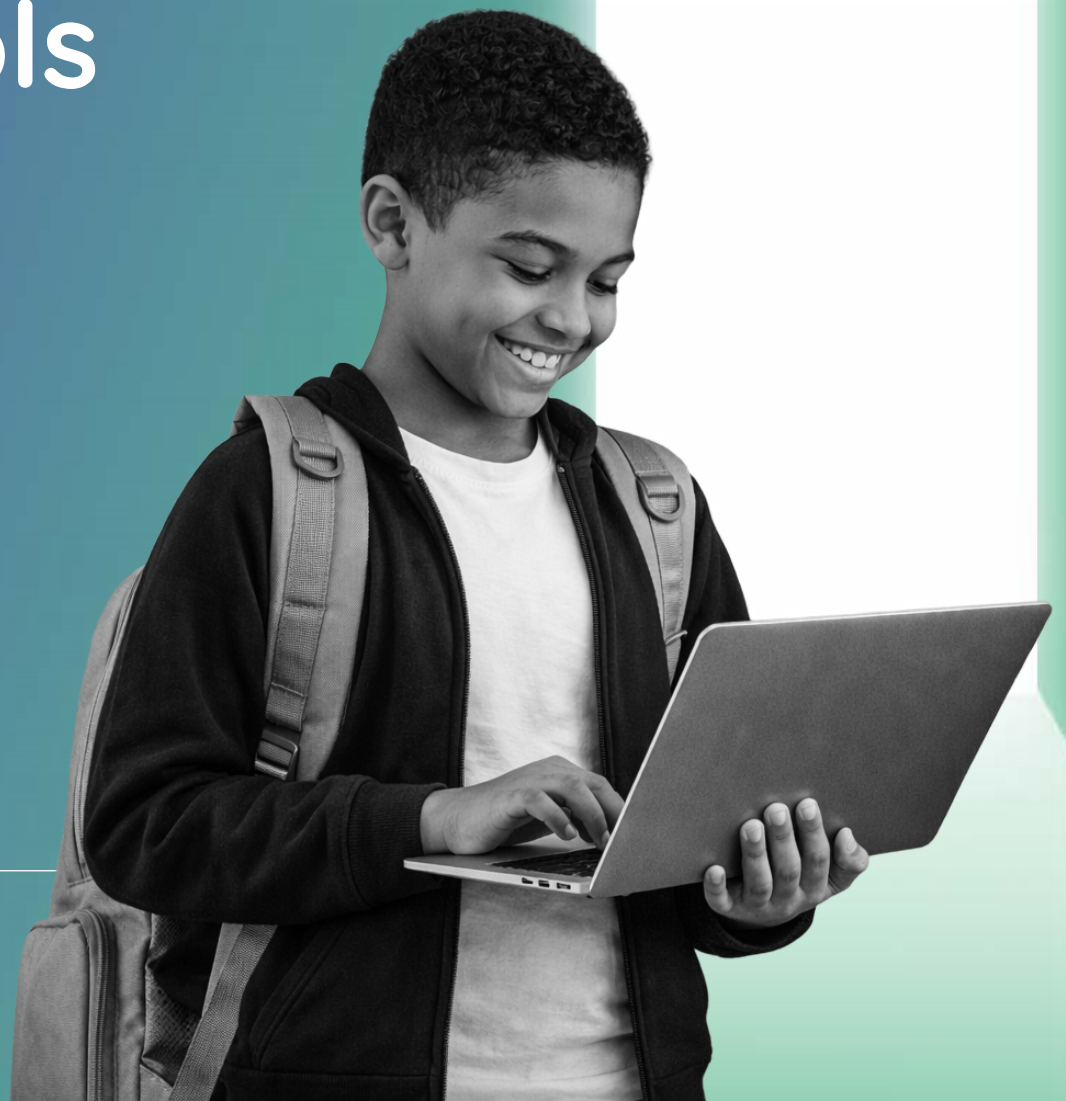


A Practical Guide Closing the Digital Safety Gaps in NZ Schools



1. Introduction

Most New Zealand schools have the foundations of digital safety in place.

Filtering is operational.

Safe Search is enforced.

Students use designated school accounts.

**These are important protections.
But they don't always tell the whole story.**

Students move constantly between devices, networks, accounts, and new tools like AI. When protection only exists in one of those places, it becomes inconsistent. And when those layers stop working together, gaps appear.

Many schools only discover those gaps after something unexpected happens.

This guide is designed to help School Leaders and Boards step back and review their current digital safety approach. The goal is simple: **move from assuming students are protected to having clear confidence that they are.**

The Challenges Facing NZ Schools Today

Digital safety has changed quickly in recent years. School leaders are navigating several shifts at once.



Legacy systems were not designed for student safety

Many schools still rely on traditional or legacy firewalls. These are important for keeping external threats out of a network, but they were never designed to manage student online behaviour or wellbeing risks.



New technologies are changing student behaviour

Tools such as AI chatbots are appearing faster than traditional filtering systems can adapt. Students can access new platforms and interactions that schools may not yet have visibility over.



The line between school and home is disappearing

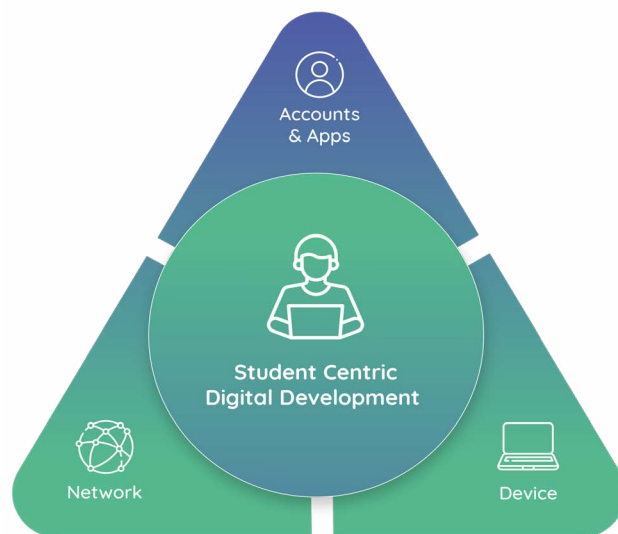
School devices increasingly travel home with students. Parents want to support safe device use, but many do not have the tools or visibility to do so. When issues arise after hours, they often return to the classroom the next day.

These realities don't mean schools are doing the wrong things. They simply highlight that digital safety now relies on more than a single layer of protection.

3 Critical Digital Safety Scenarios

Effective digital safety relies on three connected layers:

1. The **device**
2. The **network**
3. The **accounts and apps** students use



When those layers work together, protection is far stronger.

When they don't, gaps appear. Here are three common scenarios where those gaps can emerge.

Scenario 1: The “Safe Site” Gap

Moving beyond “block or allow”

Many filtering systems operate on a simple rule: if a website isn't blocked, it must be safe.

The reality

A student might be researching on a legitimate education site or running a Google image search for a simple term if a website isn't blocked, it must be safe.

Where the gap appears

Blocking the entire site would disrupt learning. But allowing it completely can expose students to inappropriate images, comments, or content hosted on that platform.

Older filtering tools force schools into an all-or-nothing decision. That creates blind spots inside otherwise trusted sites.

Schools increasingly need protection that can understand the content inside a page, not just the website address.

Scenario 2: New Technology & Hidden Chat Gaps

Why real-time visibility matters

Many people assume that if students are on the school network, the environment is safe.

The reality

Students often use everyday learning tools in unexpected ways.

A conversation that crosses a line might happen inside:

- a shared Google Doc
- a collaborative presentation
- a messaging feature within another platform
- an AI chatbot interaction

Where the gap appears

Traditional protections focus on blocking known harmful websites. They cannot always see what is happening inside shared documents or new AI platforms. This means concerning behaviour can sometimes unfold in plain sight but without visibility.

Early signals matter. Schools benefit from systems that help staff notice when something isn't right, before a situation escalates.

Closing the digital safety gaps

Scenario 3: The “Off-Network” Gap

Giving the right adults the right visibility

Many protections are still tied to the school firewall.

The reality

Students take devices home.
They connect to mobile data.
They switch networks during breaks.

Where the gap appears

If safety tools only work on the school Wi-Fi network, protection disappears the moment a student disconnects.

That can leave students navigating the internet without the same safeguards that exist at school.

Consistent digital safety increasingly means protection that travels with the device, regardless of the network being used. It also means giving parents appropriate visibility and controls so they can support safe device use after hours.

Self-Assessment: Is Your Digital Safety Approach Keeping Up?



If you want to confidently answer “Yes” to these questions, it’s time to review your current approach.

Filtering & Foundations

1. Would you like full confidence knowing that your filtering is advanced enough to prevent students from being either harmed or distracted when on devices? **Y / N**

Classroom & Teacher Visibility

2. Would your teachers benefit from being able to see what students are doing on devices during lessons, to ensure effective and safe use? **Y / N**

Community & Home Support

3. Would you like to be able to effectively support parents in dealing with issues that arise at home due to students’ challenging online behaviours? **Y / N**

Wellbeing & Early Intervention

4. Would it be valuable to receive alerts when students do things on devices that might harm them or others? **Y / N**
5. Are there students in your school that you wish would reach out for help, but they don’t? **Y / N**
6. If your students felt safe to share that they were struggling, would they appreciate you connecting with them to help? **Y / N**
7. Would having a platform that gathers the voice of every student weekly help you direct your time and energy more effectively at your school? **Y / N**
8. Would measuring the real-time impact of student engagement on wellbeing be valuable for your school and motivating for your staff? **Y / N**



Next Steps: Digital Safety Is About Clarity



Where to from here?

Digital safety isn't about adding more restrictions. It's about understanding where protection is strong and where gaps might still exist. For many schools, the first step is simply reviewing their current environment with fresh eyes.

Schools play an important role in helping students navigate the digital world safely.

That responsibility now stretches across classrooms, devices, homes, and the many platforms young people use every day. When the right protections and visibility are in place, schools, teachers, and parents can guide students with greater confidence.

If you'd like to talk through what's working, what challenges you're seeing, or how other schools are approaching digital safety, we're here to help.

Get in touch today

Whether you're reviewing your digital safety strategy or exploring ways to strengthen support for students, our team would be happy to chat.

Contact: enquiries@linewize.co.nz

Visit: www.linewize.co.nz

We're here to help.

*Raising the bar in student
digital wellbeing together.*



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



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